Sniffers

Module 08

Sniffing a Network

A packet sniffer is a type of program that monitors any bit of information entering or leaving a network. It is a type of plug-and-play wiretap device attached to a computer that eavesdrops on network traffic.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Sniffing is a technique used to **intercept data** in information security, where many of the tools that are used to secure the network can also be used by attackers to exploit and compromise the same network. The core objective of sniffing is to **steal data**, such as sensitive information, email text, etc.

Network sniffing involves intercepting network traffic between two target network nodes and capturing network packets exchanged between nodes. A **packet sniffer** is also referred to as a network monitor that is used legitimately by a network administrator to monitor the network for vulnerabilities by capturing the network traffic and should there be any issues, proceeds to troubleshoot the same.

Similarly, sniffing tools can be used by attackers in **promiscuous** mode to capture and analyze all the network traffic. Once attackers have captured the network traffic they can analyze the packets and view the **user name** and **password** information in a given network as this information is transmitted in a cleartext format. An attacker can easily intrude into a network using this login information and compromise other systems on the network.

Hence, it is very crucial for a network administrator to be familiar with **network traffic analyzers** and he or she should be able to **maintain** and **monitor** a network to detect rogue packet sniffers, MAC attacks, DHCP attacks, **ARP poisoning**, spoofing, or DNS poisoning, and know the types of information that can be detected from the captured data and use the information to keep the network running smoothly.

Lab Objectives

The objective of this lab is to familiarize students with how to sniff a network and analyze packets for any attacks on the network.

The primary objectives of this lab are to:

- Sniff the network
- Analyze incoming and outgoing packets
- Troubleshoot the network for performance

- Secure the network from attacks

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 08 Sniffing

Lab Environment

In this lab, you need:

- A web browser with an Internet connection
- Administrative privileges to run tools

Lab Duration

Time: 80 Minutes

Overview of Sniffing Network

Sniffing is performed to **collect basic information** from the target and its network. It helps to find **vulnerabilities** and select exploits for attack. It determines network information, system information, and organizational information.

TASK 1

Overview

Lab Tasks

Pick an organization that you feel is worthy of your attention. This could be an educational institution, a commercial company, or perhaps a nonprofit charity.

Recommended labs to assist you in sniffing the network:

- Sniffing the network using the **Colasoft Packet Builder**
- Sniffing the network using the **OmniPeek Network Analyzer**
- Spoofing MAC address using **SMAC**
- Sniffing the network using the **WinArpAttacker** tool
- Analyzing the network using the **Colasoft Network Analyzer**
- Sniffing passwords using **Wireshark**
- Performing man-in-the-middle attack using **Cain & Abel**
- Advanced ARP spoofing detection using **XArp**
- Detecting Systems running in promiscuous mode in a network using **PromqryUI**
- Sniffing a password from captured packets using **Sniff – O – Matic**

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure through public and free information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Lab
1

Sniffing the Network Using the OmniPeek Network Analyzer

OmniPeek is a standalone network analysis tool used to solve network problems.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

From the previous scenario, now you are aware of the importance of network sniffing. As an expert **ethical hacker** and **penetration tester**, you must have sound knowledge of sniffing network packets, performing ARP poisoning, spoofing the network, and DNS poisoning.

Lab Objectives

The objective of this lab is to reinforce concepts of network security policy, policy enforcement, and policy audits.

Lab Environment

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 08 Sniffing

In this lab, you need:

- **OmniPeek Network Analyzer** located at **D:\CEH-Tools\CEHv8 Module 08 Sniffing\Sniffing Tools\OmniPeek Network Analyzer**
- You can also download the latest version of **OmniPeek Network Analyzer** from the link http://www.wildpackets.com/products/omnipeek_network_analyzer
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- A computer running **Windows Server 2012** as host machine
- **Windows 8** running on virtual machine as target machine
- A web browser and Microsoft .NET Framework 2.0 or later
- Double-click **OmniPeek682demo.exe** and follow the wizard-driven installation steps to install **OmniPeek682demo.exe**
- **Administrative** privileges to run tools

Lab Duration

Time: 20 Minutes

Overview of OmniPeekNetwork Analyzer

OmniPeek Network Analyzer gives network engineers real-time visibility and expert analysis of each and every part of the network from a single interface, which includes Ethernet, Gigabit, 10 Gigabit, VoIP, video to remote offices, and 802.

Lab Tasks

TASK 1

Installing OmniPeek Network Analyzer

1. Install **OmniPeek Network Analyzer** on the host machine **Windows Server 2012**.
2. Launch the **Start** menu by hovering the mouse cursor on the lower left corner of the desktop.

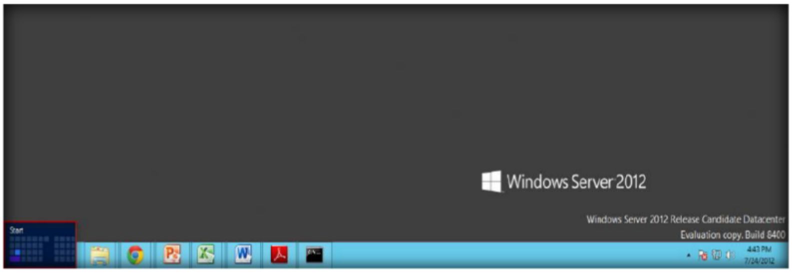

Windows Server 2012
Windows Server 2012 Release Candidate Datacenter
Evaluation copy. Build 8400
Start

FIGURE 1.1: Windows Server 2012 – Desktop view

3. Click the **WildPackets OmniPeek Demo** app in the **Start** menu to launch the tool.

OmniPeek Enterprise provides users with the visibility and analysis they need to keep Voice and Video applications and non-media applications running optimally on the network

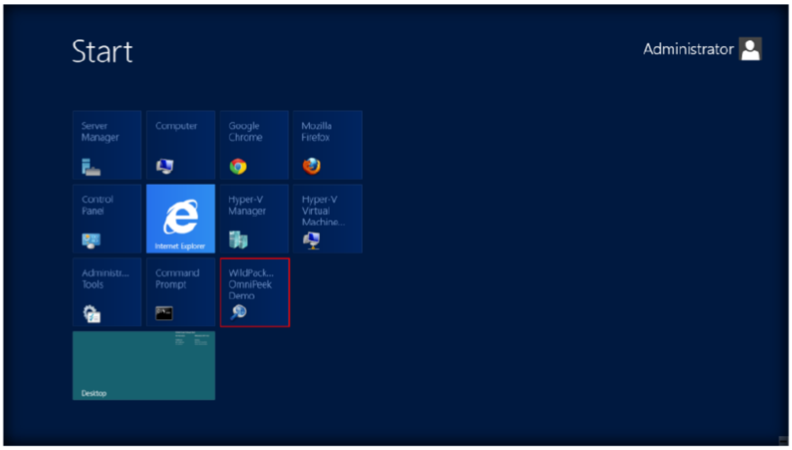

Start
Administrator
Server Manager
Computer
Google Chrome
Mozilla Firefox
Control Panel
Internet Explorer
Hyper-V Manager
Hyper-V Virtual Machine...
Administr... Tools
Command Prompt
WildPack... OmniPeek Demo
Desktop

FIGURE 1.2: Windows Server 2012 – Start menu

To deploy and maintain Voice and Video over IP successfully, you need to be able to analyze and troubleshoot media traffic simultaneously with the network the media traffic is running on

4. The main window of **WildPackets OmniPeek Demo** appears, as shown in the following screenshot.

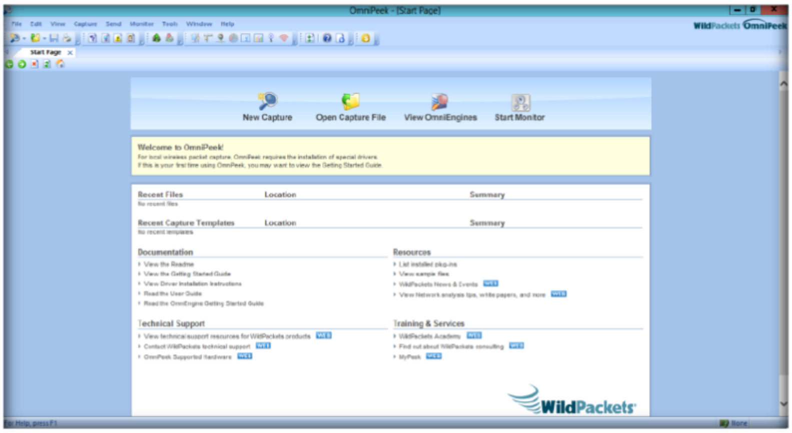

OmniPeek - [Start Page]
New Capture
Open Capture File
View OmniEngines
Start Monitor
Welcome to OmniPeek!
Recent Files
Recent Capture Templates
Documentation
Resources
Technical Support
Training & Services
WildPackets

FIGURE 1.3: OmniPeek main screen

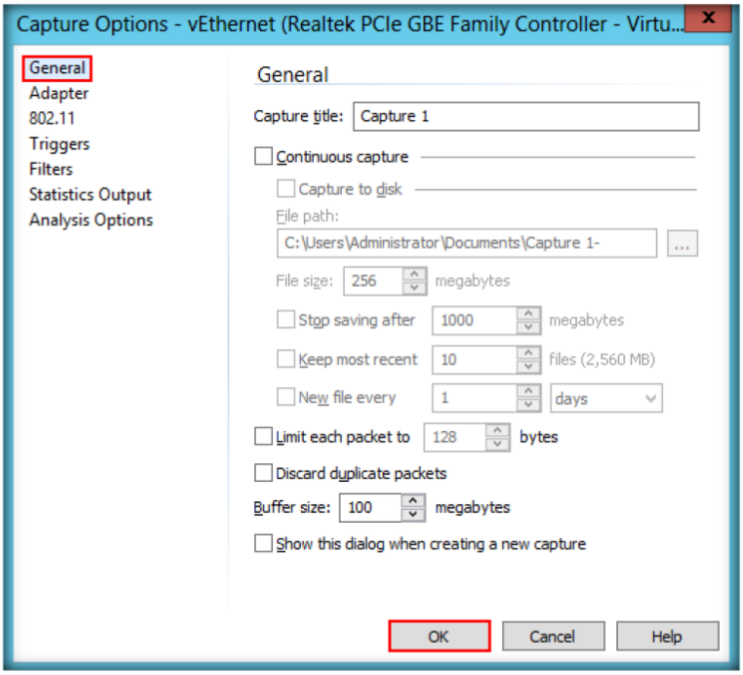
5. **Launch** Windows 8 Virtual Machine.

TASK 2

Starting New Capture

6. Now, in **Windows Server 2012** create an OmniPeek capture window as follows:
   a. Click the **New Capture** icon on the main screen of OmniPeek.
   b. View the **General** options in the **OmniPeek Capture Options** dialog box when it appears.
   c. Leave the default general settings and click **OK**.

OmniPeek Network Analyzer offers real-time high-level view of the entire network, expert analyses, and drill-down to packets, during capture.


Capture Options - vEthernet (Realtek PCIe GBE Family Controller - Virtu...
General
Adapter
802.11
Triggers
Filters
Statistics Output
Analysis Options
General
OK
Cancel
Help

Capture title: Capture 1

☐ Continuous capture

☐ Capture to disk

File path: C:\Users\Administrator\Documents\Capture 1-

File size: 256 megabytes

☐ Stop saving after 1000 megabytes

☐ Keep most recent 10 files (2,560 MB)

☐ New file every 1 days

☐ Limit each packet to 128 bytes

☐ Discard duplicate packets

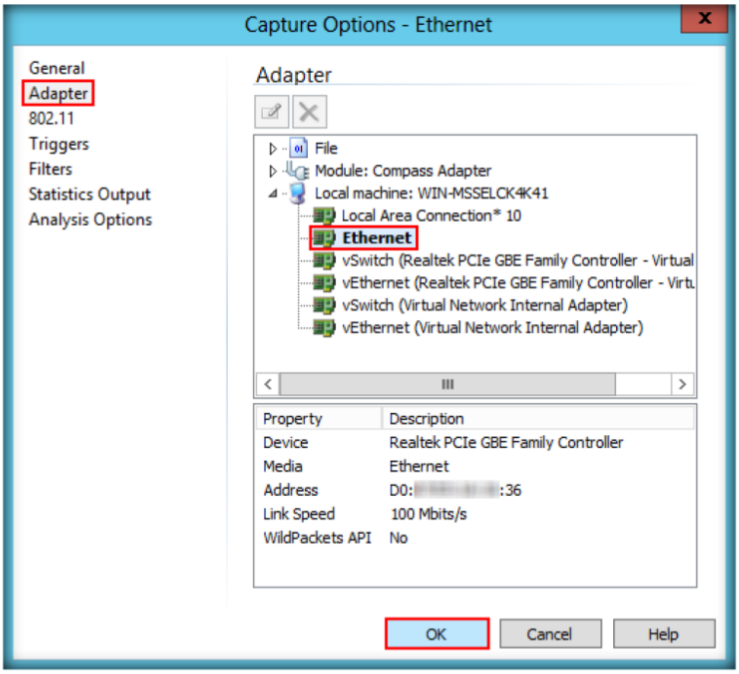
Buffer size: 100 megabytes

☐ Show this dialog when creating a new capture

FIGURE 1.4: OmniPeek capture options - General

d. Click **Adapter** and select **Ethernet** in the list for **Local machine**. Click **OK**.

Network Coverage: With the Ethernet, Gigabit, 10G, and wireless capabilities, you can now effectively monitor and troubleshoot services running on your entire network. Using the same solution for troubleshooting wired and wireless networks reduces the total cost of ownership and illuminates network problems that would otherwise be difficult to detect.


Capture Options - Ethernet
General
Adapter
802.11
Triggers
Filters
Statistics Output
Analysis Options
Adapter
OK
Cancel
Help

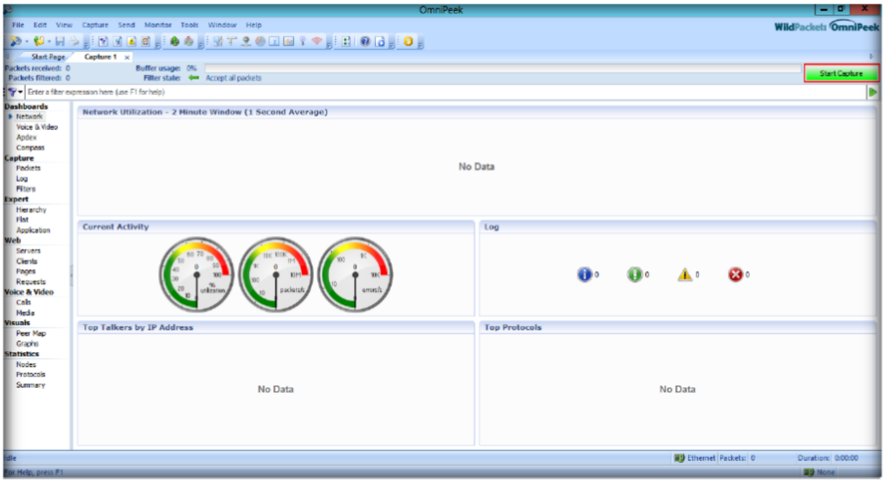
File
Module: Compass Adapter
Local machine: WIN-MSSELCK4K41
Local Area Connection* 10
Ethernet
vSwitch (Realtek PCIe GBE Family Controller - Virtual
vEthernet (Realtek PCIe GBE Family Controller - Virtu
vSwitch (Virtual Network Internal Adapter)
vEthernet (Virtual Network Internal Adapter)

Property	Description
Device	Realtek PCIe GBE Family Controller
Media	Ethernet
Address	D0:[redacted]:36
Link Speed	100 Mbits/s
WildPackets API	No

FIGURE 1.5: OmniPeek capture options - Adapter

7. Now, click **Start Capture** to begin capturing packets. The **Start Capture** tab changes to **Stop Capture** and traffic statistics begin to populate the **Network Dashboard** in the capture window of OmniPeek.

Dashboards display important data that every network engineer needs to know regarding the network without spending lots of time analyzing the captured data.


OmniPeek
File Edit View Capture Send Monitor Tools Window Help
WildPackets OmniPeek
Start Page
Capture 1
Start Capture
Dashboards
Network
Voice & Video
Apdex
Compass
Capture
Packets
Log
Filters
Expert
Hierarchy
Flat
Application
Web
Servers
Clients
Pages
Requests
Voice & Video
Calls
Media
Visuals
Peer Map
Graphs
Statistics
Nodes
Protocols
Summary
Network Utilization - 2 Minute Window (1 Second Average)
No Data
Current Activity
Log
Top Talkers by IP Address
No Data
Top Protocols
No Data

Packets received: 0
Packets filtered: 0
Buffer usage: 0%
Filter state: Accept all packets
Enter a filter expression here (use F1 for help)

FIGURE 1.6: OmniPeek creating a capture window

OmniPeek Professional expands the capabilities of OmniPeek Basic, extending its reach to all small businesses and corporate workgroups, regardless of the size of the network or the number of employees. OmniPeek Professional provides support for multiple network interfaces while still supporting up to 2 Omni Engines acting as both a full-featured network analyzer and console for remote network analysis.

8. The captured statistical analysis of the data is displayed on the **Capture** tab of the navigation bar.

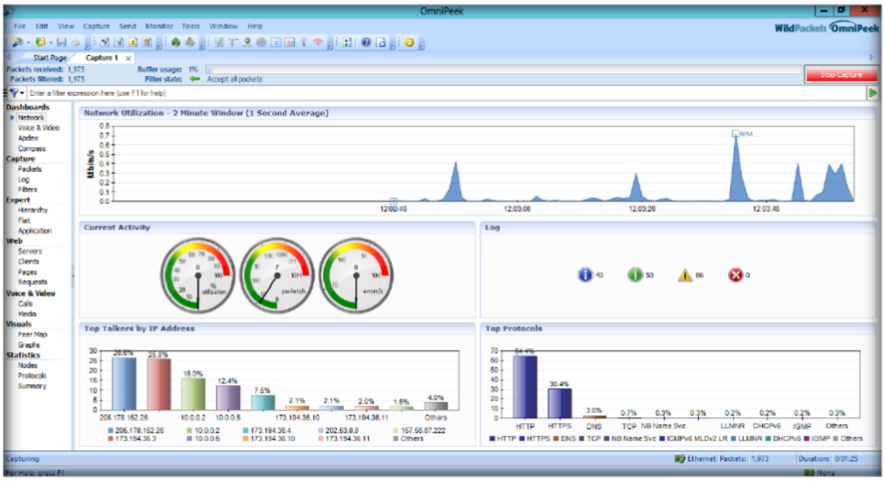
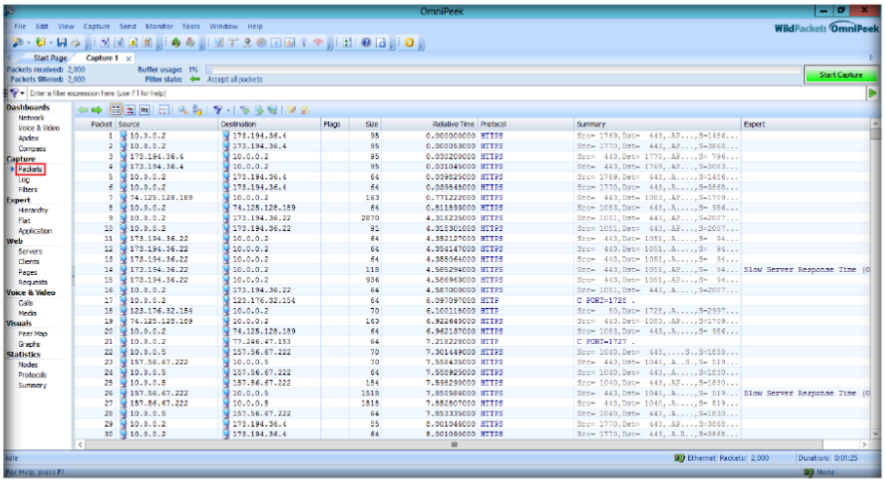

OmniPeek
File Edit View Capture Send Monitor Tools Window Help
WildPackets OmniPeek
Start Page
Capture 1
Packets received: 1,973
Packets filtered: 1,973
Buffer usage: 1%
Filter state: Accept all packets
Stop Capture
Enter a filter expression here (use F1 for help)
Dashboards
Network
Voice & Video
Apdex
Compass
Capture
Packets
Log
Filters
Expert
Hierarchy
Flat
Application
Web
Servers
Clients
Pages
Requests
Voice & Video
Calls
Media
Visuals
Peer Map
Graphs
Statistics
Nodes
Protocols
Summary
Network Utilization - 2 Minute Window (1 Second Average)
Mbits/s
MAX
12:02:48
12:03:08
12:03:28
12:03:48
Current Activity
utilization
packets/s
errors/s
Log
43
50
86
0
Top Talkers by IP Address
26.6%
25.3%
15.0%
12.4%
7.6%
2.1%
2.1%
2.0%
1.6%
4.0%
205.178.152.28
10.0.0.2
10.0.0.5
173.194.36.10
173.194.36.11
Others
173.194.36.3
173.194.36.4
202.63.8.8
157.56.67.222
Top Protocols
54.4%
30.4%
3.0%
0.7%
0.3%
HTTP
HTTPS
DNS
TCP
NB Name Svc
ICMPv6 MLDv2 LR
LLMNR
DHCPv6
IGMP
Others
Capturing
Ethernet
Packets: 1,973
Duration: 0:01:25
For Help, press F1

FIGURE 1.7: OmniPeek statistical analysis of the data

9. To view the captured packets, select **Packets** in a **Capture** section of the **Dashboard** in the left pane of the window.


OmniPeek
File Edit View Capture Send Monitor Tools Window Help
WildPackets OmniPeek
Start Page
Capture 1
Packets received: 2,000
Packets filtered: 2,000
Buffer usage: 1%
Filter state: Accept all packets
Start Capture
Enter a filter expression here (use F1 for help)
Dashboards
Network
Voice & Video
Apdex
Compass
Capture
Packets
Log
Filters
Expert
Hierarchy
Flat
Application
Web
Servers
Clients
Pages
Requests
Voice & Video
Calls
Media
Visuals
Peer Map
Graphs
Statistics
Nodes
Protocols
Summary
Idle
Ethernet
Packets: 2,000
Duration: 0:01:25
For Help, press F1
None

Packet	Source	Destination	Flags	Size	Relative Time	Protocol	Summary	Expert
1	10.0.0.2	173.194.36.4		95	0.000000000	HTTPS	Src= 1769,Dst= 443,.AP....,S=1486...	
2	10.0.0.2	173.194.36.4		95	0.000053000	HTTPS	Src= 1770,Dst= 443,.AP....,S=3868...	
3	173.194.36.4	10.0.0.2		95	0.030209000	HTTPS	Src= 443,Dst= 1770,.AP....,S= 796...	
4	173.194.36.4	10.0.0.2		95	0.031045000	HTTPS	Src= 443,Dst= 1769,.AP....,S=3083...	
5	10.0.0.2	173.194.36.4		64	0.039825000	HTTPS	Src= 1769,Dst= 443,.A.....,S=1486...	
6	10.0.0.2	173.194.36.4		64	0.039848000	HTTPS	Src= 1770,Dst= 443,.A.....,S=3868...	
7	74.125.128.189	10.0.0.2		163	0.771222000	HTTPS	Src= 443,Dst= 1083,.AP....,S=1709...	
8	10.0.0.2	74.125.128.189		64	0.811893000	HTTPS	Src= 1083,Dst= 443,.A.....,S= 956...	
9	10.0.0.2	173.194.36.22		2870	4.318235000	HTTPS	Src= 1051,Dst= 443,.AP....,S=2007...	
10	10.0.0.2	173.194.36.22		91	4.318301000	HTTPS	Src= 1051,Dst= 443,.AP....,S=2007...	
11	173.194.36.22	10.0.0.2		64	4.352127000	HTTPS	Src= 443,Dst= 1051,.A.....,S= 94...	
12	173.194.36.22	10.0.0.2		64	4.354147000	HTTPS	Src= 443,Dst= 1051,.A.....,S= 94...	
13	173.194.36.22	10.0.0.2		64	4.355064000	HTTPS	Src= 443,Dst= 1051,.A.....,S= 94...	
14	173.194.36.22	10.0.0.2		118	4.585294000	HTTPS	Src= 443,Dst= 1051,.AP....,S= 94...	Slow Server Response Time (0
15	173.194.36.22	10.0.0.2		936	4.586963000	HTTPS	Src= 443,Dst= 1051,.AP....,S= 94...	
16	10.0.0.2	173.194.36.22		64	4.587000000	HTTPS	Src= 1051,Dst= 443,.A.....,S=2007...	
17	10.0.0.2	123.176.32.154		64	6.097097000	HTTP	C PORT=1728 .	
18	123.176.32.154	10.0.0.2		70	6.100118000	HTTP	Src= 80,Dst= 1728,.A.....,S=2997...	
19	74.125.128.189	10.0.0.2		163	6.922645000	HTTPS	Src= 443,Dst= 1083,.AP....,S=1709...	
20	10.0.0.2	74.125.128.189		64	6.962137000	HTTPS	Src= 1083,Dst= 443,.A.....,S= 956...	
21	10.0.0.2	77.246.47.153		64	7.218228000	HTTP	C PORT=1727 .	
22	10.0.0.5	157.56.67.222		70	7.301449000	HTTPS	Src= 1040,Dst= 443,....S.,S=1830...	
23	157.56.67.222	10.0.0.5		70	7.558435000	HTTPS	Src= 443,Dst= 1040,.A..S.,S= 519...	
24	10.0.0.5	157.56.67.222		64	7.558925000	HTTPS	Src= 1040,Dst= 443,.A.....,S=1830...	
25	10.0.0.5	157.56.67.222		184	7.598290000	HTTPS	Src= 1040,Dst= 443,.AP....,S=1830...	
26	157.56.67.222	10.0.0.5		1518	7.850586000	HTTPS	Src= 443,Dst= 1040,.A.....,S= 519...	Slow Server Response Time (0
27	157.56.67.222	10.0.0.5		1518	7.852807000	HTTPS	Src= 443,Dst= 1040,.A.....,S= 519...	
28	10.0.0.5	157.56.67.222		64	7.853335000	HTTPS	Src= 1040,Dst= 443,.A.....,S=1830...	
29	10.0.0.2	173.194.36.4		85	8.001046000	HTTPS	Src= 1770,Dst= 443,.AP....,S=3868...	
30	10.0.0.2	173.194.36.4		64	8.001090000	HTTPS	Src= 1770,Dst= 443,.A.R...,S=3868...	

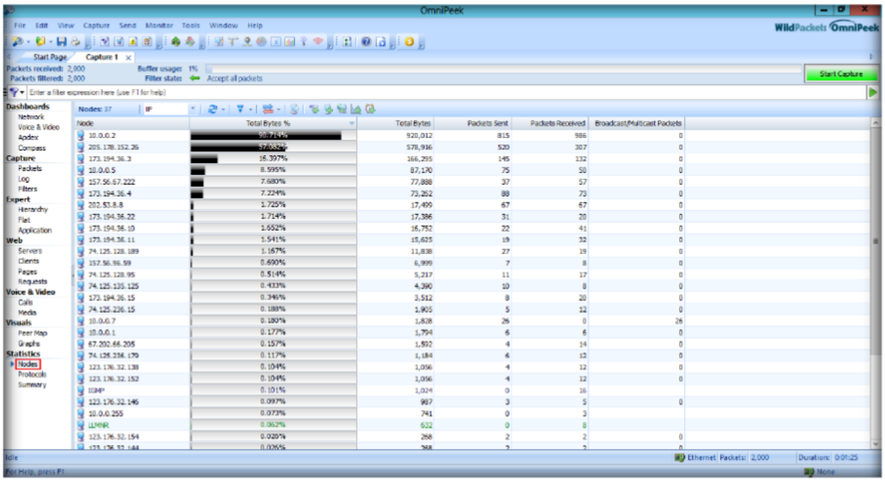
FIGURE 1.8: OmniPeek displaying Packets captured

The OmniPeek Peer Map shows all communicating nodes within your network and is drawn as a vertically-oriented ellipse, able to grow to the size necessary. It is easy to read the maps, the thicker the line between nodes, the greater the traffic; the bigger the dot, the more traffic through that node. The number of nodes displayed can also be limited to the busiest and/or active nodes, or to any OmniPeek filters that may be in use.

10. Similarly, you can view **Log**, **Filters**, **Hierarchy**, and **Peer Map** by selecting the respective options in the **Dashboard**.

11. You can view the **Nodes** and **Protocols** from the **Statistics** section of the Dashboard.

On-the-Fly Filters: You shouldn't have to stop your analysis to change what you're looking at. OmniPeek enables you to create filters and apply them immediately. The WildPackets "select related" feature selects the packets relevant to a particular node, protocol, conversation, or expert diagnosis, with a simple right click of the mouse.


OmniPeek
File Edit View Capture Send Monitor Tools Window Help
WildPackets OmniPeek
Start Page
Capture 1
Start Capture
Dashboards
Network
Voice & Video
Apdex
Compass
Capture
Packets
Log
Filters
Expert
Hierarchy
Flat
Application
Web
Servers
Clients
Pages
Requests
Voice & Video
Calls
Media
Visuals
Peer Map
Graphs
Statistics
Nodes
Protocols
Summary
Idle
Ethernet
For Help, press F1
None

Packets received: 2,000
Packets filtered: 2,000
Buffer usage: 1%
Filter state: Accept all packets
Enter a filter expression here (use F1 for help)
Nodes: 37
IP

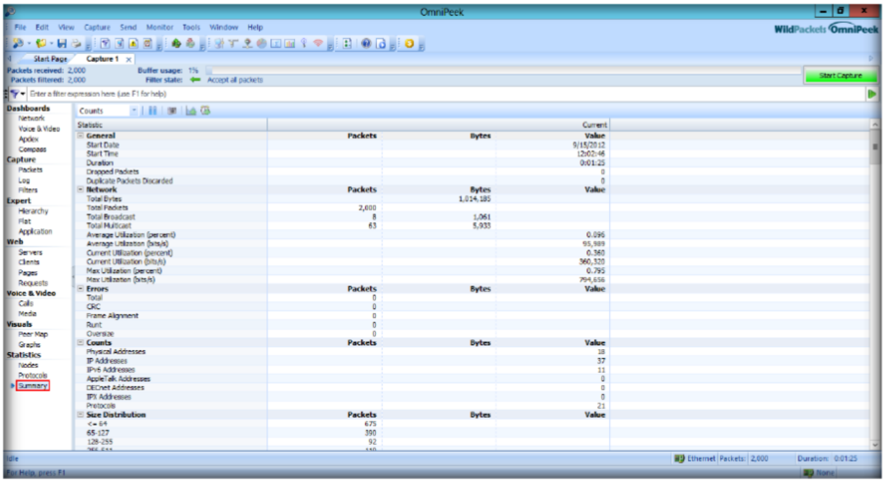
Node	Total Bytes %	Total Bytes	Packets Sent	Packets Received	Broadcast/Multicast Packets
10.0.0.2	90.714%	920,012	815	986	0
205.178.152.26	57.082%	578,916	520	307	0
173.194.36.3	16.397%	166,295	145	132	0
10.0.0.5	8.595%	87,170	75	50	0
157.56.67.222	7.680%	77,888	37	57	0
173.194.36.4	7.224%	73,262	88	73	0
202.53.8.8	1.725%	17,499	67	67	0
173.194.36.22	1.714%	17,386	31	20	0
173.194.36.10	1.652%	16,752	22	41	0
173.194.36.11	1.541%	15,625	19	32	0
74.125.128.189	1.167%	11,838	27	19	0
157.56.96.59	0.690%	6,999	7	8	0
74.125.128.95	0.514%	5,217	11	17	0
74.125.135.125	0.433%	4,390	10	8	0
173.194.36.15	0.346%	3,512	8	20	0
74.125.236.15	0.188%	1,905	5	12	0
10.0.0.7	0.180%	1,828	26	0	26
10.0.0.1	0.177%	1,794	6	6	0
67.202.66.205	0.157%	1,592	4	14	0
74.125.236.170	0.117%	1,184	6	12	0
123.176.32.138	0.104%	1,056	4	12	0
123.176.32.152	0.104%	1,056	4	12	0
IGMP	0.101%	1,024	0	16	
123.176.32.146	0.097%	987	3	5	0
10.0.0.255	0.073%	741	0	3	
LLMNR	0.062%	632	0	8	
123.176.32.154	0.026%	268	2	2	0

Packets: 2,000
Duration: 0:01:25

FIGURE 1.9: OmniPeek statistical reports of Nodes

12. You can view a complete **Summary** of your network from the **Statistics** section of the **Dashboard**.

Alarms and Notifications: Using its advanced alarms and notifications, OmniPeek uncovers hard-to-diagnose network problems and notifies the occurrence of issues immediately. OmniPeek alarms query a specified monitor statistics function once per second, testing for user-specified problem and resolution conditions.


OmniPeek
File Edit View Capture Send Monitor Tools Window Help
WildPackets OmniPeek
Start Page
Capture 1
Start Capture
Dashboards
Network
Voice & Video
Apdex
Compass
Capture
Packets
Log
Filters
Expert
Hierarchy
Flat
Application
Web
Servers
Clients
Pages
Requests
Voice & Video
Calls
Media
Visuals
Peer Map
Graphs
Statistics
Nodes
Protocols
Summary
Idle
Ethernet
For Help, press F1
None

Packets received: 2,000
Packets filtered: 2,000
Buffer usage: 1%
Filter state: Accept all packets
Enter a filter expression here (use F1 for help)
Counts

Statistic			Current
General	**Packets**	**Bytes**	**Value**
Start Date			9/15/2012
Start Time			12:02:46
Duration			0:01:25
Dropped Packets			0
Duplicate Packets Discarded			0
Network	**Packets**	**Bytes**	**Value**
Total Bytes		1,014,185	
Total Packets	2,000		
Total Broadcast	8	1,061	
Total Multicast	63	5,933	
Average Utilization (percent)			0.096
Average Utilization (bits/s)			95,989
Current Utilization (percent)			0.360
Current Utilization (bits/s)			360,320
Max Utilization (percent)			0.795
Max Utilization (bits/s)			794,656
Errors	**Packets**	**Bytes**	**Value**
Total	0		
CRC	0		
Frame Alignment	0		
Runt	0		
Oversize	0		
Counts	**Packets**	**Bytes**	**Value**
Physical Addresses			18
IP Addresses			37
IPv6 Addresses			11
AppleTalk Addresses			0
DECnet Addresses			0
IPX Addresses			0
Protocols			21
Size Distribution	**Packets**	**Bytes**	**Value**
<= 64	675		
65-127	390		
128-255	92		

Packets: 2,000
Duration: 0:01:25

FIGURE 1.10: OmniPeek Summary details

13. To **save** the result, select **File→Save Report**.

Using OmniPeek's local capture capabilities, centralized console distributes OmniEngine intelligent software probes, Omnipliance®, TimeLine™ network recorders, and Expert Analysis.

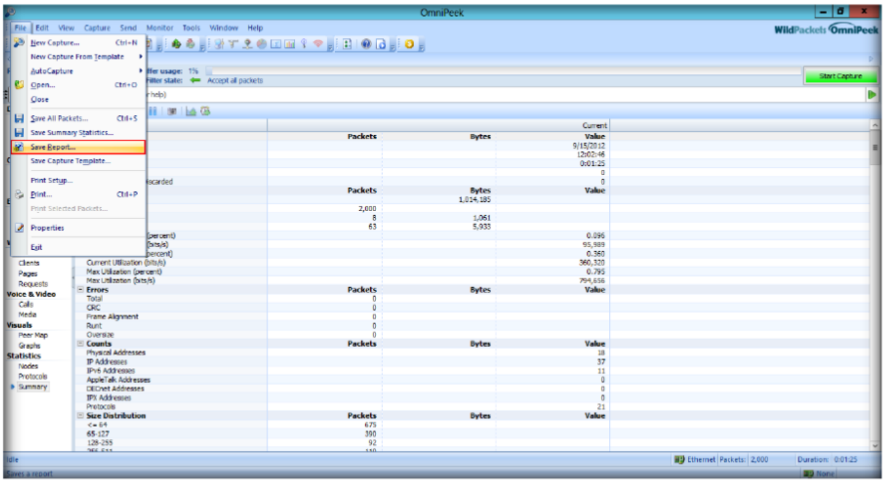
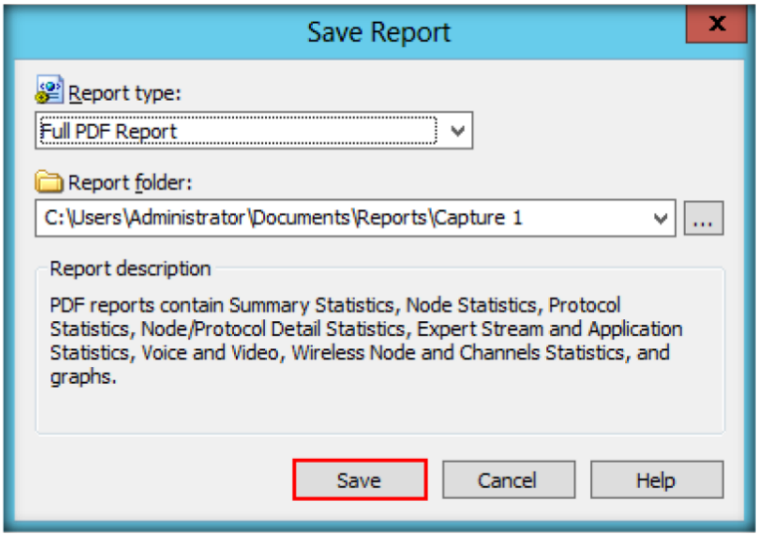

OmniPeek
File Edit View Capture Send Monitor Tools Window Help
New Capture... Ctrl+N
New Capture From Template
AutoCapture
Open... Ctrl+O
Close
Save All Packets... Ctrl+S
Save Summary Statistics...
Save Report...
Save Capture Template...
Print Setup...
Print... Ctrl+P
Print Selected Packets...
Properties
Exit
Start Capture
WildPackets OmniPeek

FIGURE 1.11: OmniPeek saving the results

14. Choose the format of the report type from the **Save Report** window and then click **Save**.

Engineers can monitor their entire network, rapidly troubleshoot faults, and fix problems to maximize network uptime and user satisfaction.


Save Report
Save
Cancel
Help

Report type: Full PDF Report

Report folder: C:\Users\Administrator\Documents\Reports\Capture 1

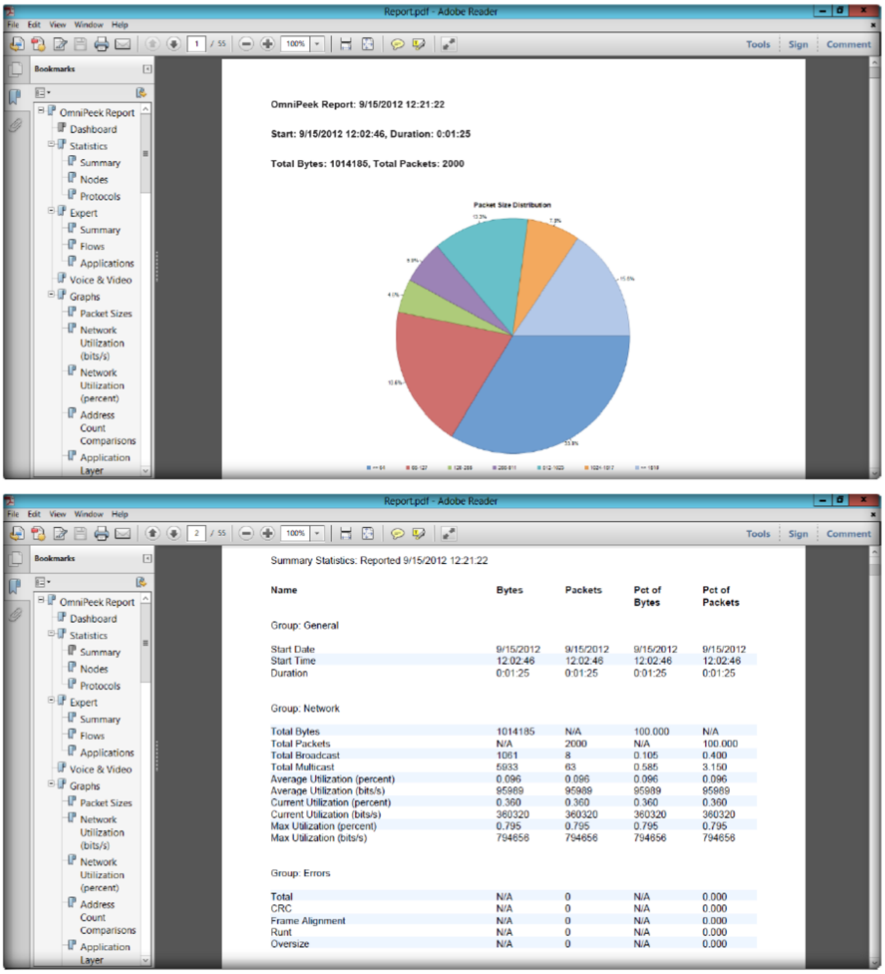
Report description

PDF reports contain Summary Statistics, Node Statistics, Protocol Statistics, Node/Protocol Detail Statistics, Expert Stream and Application Statistics, Voice and Video, Wireless Node and Channels Statistics, and graphs.

FIGURE 1.12: OmniPeek Selecting the Report format

FIGURE 1.12: OmniPeek Selecting the Report format

15. The report can be viewed as a PDF.


Report.pdf - Adobe Reader
File Edit View Window Help
1 / 55
100%
Tools
Sign
Comment
Bookmarks
OmniPeek Report
Dashboard
Statistics
Summary
Nodes
Protocols
Expert
Summary
Flows
Applications
Voice & Video
Graphs
Packet Sizes
Network Utilization (bits/s)
Network Utilization (percent)
Address Count Comparisons
Application Layer
Packet Size Distribution
13.3%
7.3%
15.6%
33.8%
Report.pdf - Adobe Reader
2 / 55

OmniPeek Report: 9/15/2012 12:21:22

Start: 9/15/2012 12:02:46, Duration: 0:01:25

Total Bytes: 1014185, Total Packets: 2000

Summary Statistics: Reported 9/15/2012 12:21:22

Name	Bytes	Packets	Pct of Bytes	Pct of Packets
Group: General				
Start Date	9/15/2012	9/15/2012	9/15/2012	9/15/2012
Start Time	12:02:46	12:02:46	12:02:46	12:02:46
Duration	0:01:25	0:01:25	0:01:25	0:01:25
Group: Network				
Total Bytes	1014185	N/A	100.000	N/A
Total Packets	N/A	2000	N/A	100.000
Total Broadcast	1061	8	0.105	0.400
Total Multicast	5933	63	0.585	3.150
Average Utilization (percent)	0.096	0.096	0.096	0.096
Average Utilization (bits/s)	95989	95989	95989	95989
Current Utilization (percent)	0.360	0.360	0.360	0.360
Current Utilization (bits/s)	360320	360320	360320	360320
Max Utilization (percent)	0.795	0.795	0.795	0.795
Max Utilization (bits/s)	794656	794656	794656	794656
Group: Errors				
Total	N/A	0	N/A	0.000
CRC	N/A	0	N/A	0.000
Frame Alignment	N/A	0	N/A	0.000
Runt	N/A	0	N/A	0.000
Oversize	N/A	0	N/A	0.000

FIGURE 1.13: OmniPeek Report in PDF format

Compass Interactive Dashboard offers both real-time and post-capture monitoring of high-level network statistics with drill down capability into packets for the selected time range. Using the Compass dashboard, multiple files can be aggregated and analyzed simultaneously.

Lab Analysis

Analyze and document the results related to the lab exercise.

Tool/Utility	Information Collected/Objectives Achieved
OmniPeek Network Analyzer	**Network Information:** ▪ Network Utilization ▪ Current Activity ▪ Log ▪ Top Talkers by IP Address ▪ Top Protocols
	Packets Information: ▪ Source ▪ Destination ▪ Size ▪ Protocol
	Nodes Statistics: ▪ Total Bytes for a Node ▪ Packets Sent ▪ Packets Received ▪ Broadcast/Multicast Packets
	Summary includes Information such as: ▪ General ▪ Network ▪ Errors ▪ Counts ▪ Size Distribution

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Analyze what 802.11n adapters are supported in OmniPeek Network Analyzer.
2. Determine how you can use the OmniPeek Analyzer to assist with firewall rules.
3. Evaluate how you create a filter to span multiple ports.

Internet Connection Required	
☐ **Yes**	☑ No
Platform Supported	
☑ **Classroom**	☑ iLabs

Lab
2

Spoofing MAC Address Using SMAC

SMAC is a powerful and easy-to-use tool that is a MAC address changer (spoofer). The tool can activate a new MAC address right after changing it automatically.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

In the previous lab you learned how to use OmniPeek Network Analyzer to capture network packets and analyze the packets to determine if any vulnerability is present in the network. If an attacker is able to capture the network packets using such tools, he or she can gain information such as packet source and destination, total packets sent and received, errors, etc., which will allow the attacker to analyze the captured packets and exploit all the computers in a network.

If an administrator does not have a certain level of working skills of a packet sniffer, it is really hard to defend intrusions. So as an expert **ethical hacker** and **penetration tester**, you must spoof MAC addresses, sniff network packets, and perform ARP poisoning, network spoofing, and DNS poisoning. In this lab you will examine how to spoof a MAC address to remain unknown to an attacker.

Lab Objectives

The objective of this lab is to reinforce concepts of network security policy, policy enforcement, and policy audits.

In this lab, you will learn how to spoof a MAC address.

Lab Environment

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 08 Sniffing

In the lab, you need:

- **SMAC** located at **D:\CEH-Tools\CEHv8 Module 08 Sniffing\MAC Spoofing Tools\SMAC**
- You can also download the latest version of **SMAC** from the link http://www.klcconsulting.net/smac/default.htm#smac27
- If you decide to download the **latest version**, then screenshots shown in the lab might differ

- A computer running **Windows Server 2012** as Host and Windows Server 2008 as Victim Machine
- Double-click **smac27beta_setup.exe** and follow the wizard-driven installation steps to install SMAC
- **Administrative** privileges to run tools
- A web browser with Internet access

Lab Duration

Time: 10 Minutes

Overview of SMAC

SMAC is a powerful yet easy-to-use and intuitive Windows MAC address modifying utility (MAC address spoofing) which allows users to change MAC addresses for almost any Network Interface Cards (NICs) on the Windows 2003systems, regardless of whether the manufacturers allow this option.

Spoofing a MAC protects **personal** and **individual privacy**. Many organizations track wired or wireless network users via their MAC addresses. In addition, there are more and more **Wi-Fi wireless** connections available these days and wireless networks use MAC addresses to **communicate**. Wireless network security and privacy is all about MAC addresses.

Spoofing is carried out to perform security **vulnerability testing**, penetration testing on MAC address-based **authentication** and **authorization** systems, i.e. wireless access points. (Disclaimer: Authorization to perform these tests must be obtained from the system's owner(s)).

Lab Tasks

1. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

SMAC works on the Network Interface Card (NIC), which is on the Microsoft hardware compatibility list (HCL).

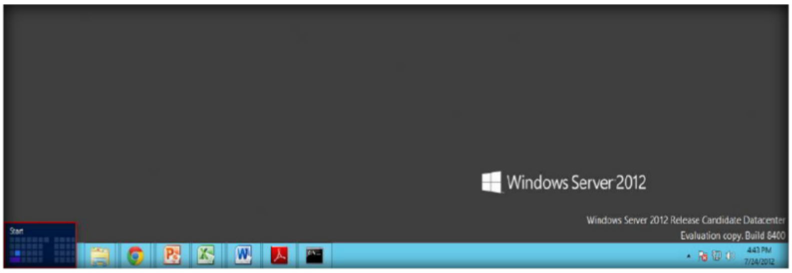

Windows Server 2012
Windows Server 2012 Release Candidate Datacenter
Evaluation copy. Build 8400
Start

FIGURE 2.1: Windows Server 2012 – Desktop view

2. Click the **SMAC 2.7** app in the **Start** menu to launch the tool.

When you start SMAC program, you must start it as the administrator. You could do this by right click on the SMAC program icon and click on "Run as Administrator if not logged in as an administrator.

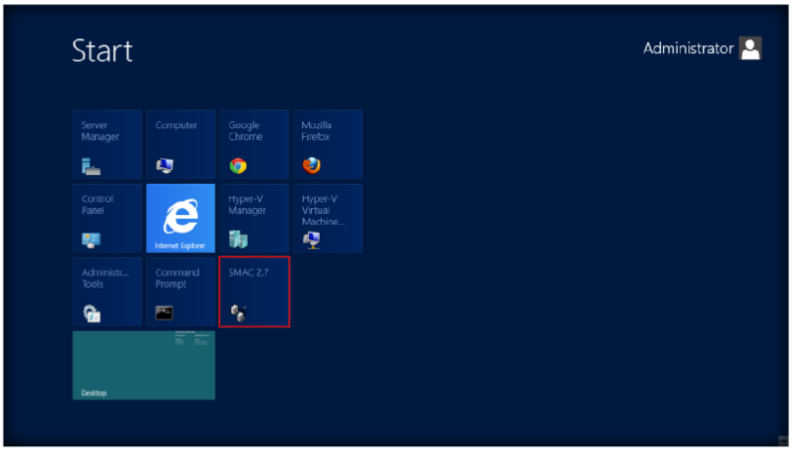
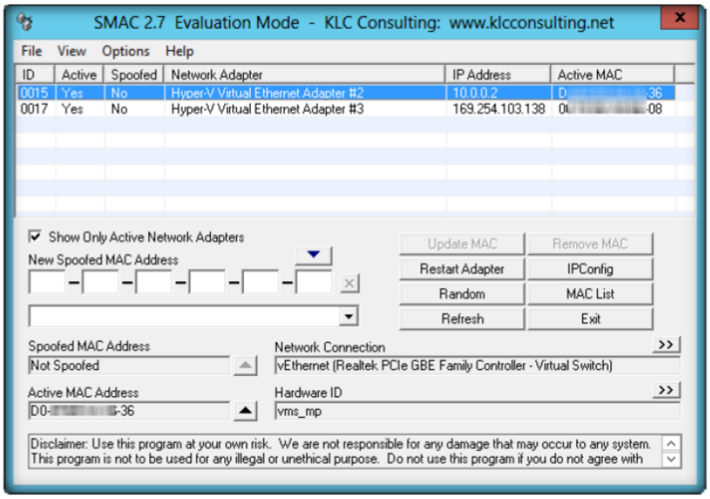

Start
Administrator
Server Manager
Computer
Google Chrome
Mozilla Firefox
Control Panel
Internet Explorer
Hyper-V Manager
Hyper-V Virtual Machine...
Administr... Tools
Command Prompt
SMAC 2.7
Desktop

FIGURE 2.2: Windows Server 2012 – Start menu

TASK 1

Spoofing MAC Address

3. The **SMAC** main screen appears. Choose a network adapter to spoof a MAC address.


SMAC 2.7 Evaluation Mode - KLC Consulting: www.klcconsulting.net
File
View
Options
Help
Update MAC
Remove MAC
Restart Adapter
IPConfig
Random
MAC List
Refresh
Exit
>>
>>

ID	Active	Spoofed	Network Adapter	IP Address	Active MAC
0015	Yes	No	Hyper-V Virtual Ethernet Adapter #2	10.0.0.2	D[redacted]36
0017	Yes	No	Hyper-V Virtual Ethernet Adapter #3	169.254.103.138	0[redacted]08

☑ Show Only Active Network Adapters

New Spoofed MAC Address

Spoofed MAC Address: Not Spoofed

Network Connection: vEthernet (Realtek PCIe GBE Family Controller - Virtual Switch)

Active MAC Address: D0-[redacted]-36

Hardware ID: vms_mp

Disclaimer: Use this program at your own risk. We are not responsible for any damage that may occur to any system. This program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with

FIGURE 2.3: SMAC main screen

SMAC helps people to protect their privacy by hiding their real MAC Addresses in the widely available Wi-Fi Wireless Network.

4. To generate a random MAC address, **Random**.

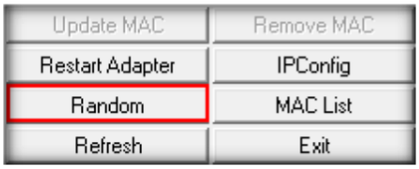
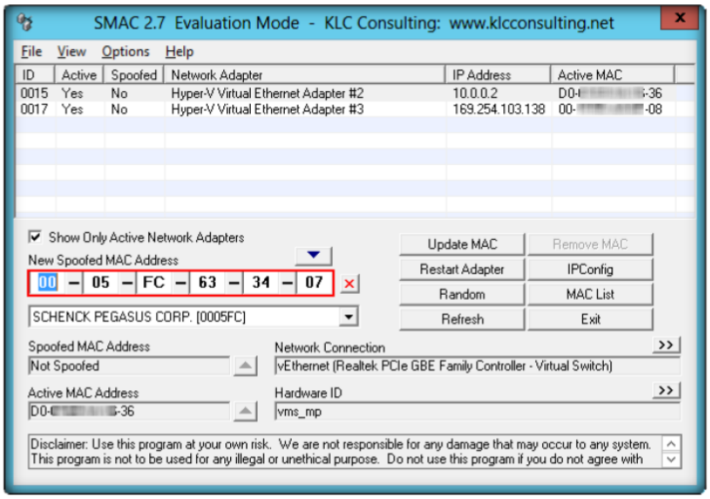

Update MAC
Remove MAC
Restart Adapter
IPConfig
Random
MAC List
Refresh
Exit

FIGURE 2.4: SMAC Random button to generate MAC addresses

5. Clicking the **Random** button also inputs the **New Spoofed MAC Address** to simply MAC address spoofing.

SMAC also helps Network and IT Security professionals to troubleshoot network problems, test Intrusion Detection / Prevention Systems (IDS/IPS,) test Incident Response plans, build high-availability solutions, recover (MAC Address based) software licenses, and etc.



ID	Active	Spoofed	Network Adapter	IP Address	Active MAC
0015	Yes	No	Hyper-V Virtual Ethernet Adapter #2	10.0.0.2	D0-[redacted]-36
0017	Yes	No	Hyper-V Virtual Ethernet Adapter #3	169.254.103.138	00-[redacted]-08

☑ Show Only Active Network Adapters

New Spoofed MAC Address: 00 – 05 – FC – 63 – 34 – 07

SCHENCK PEGASUS CORP. [0005FC]

Spoofed MAC Address: Not Spoofed

Network Connection: vEthernet (Realtek PCIe GBE Family Controller - Virtual Switch)

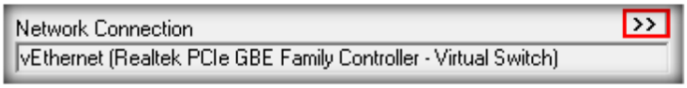
Active MAC Address: D0-[redacted]-36

Hardware ID: vms_mp

Disclaimer: Use this program at your own risk. We are not responsible for any damage that may occur to any system. This program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with

FIGURE 2.5: SMAC selecting a new spoofed MAC address

6. The Network Connection or Adapter display their respective names.
7. Click the forward arrow button in **Network Connection** to display the **Network Adapter** information.

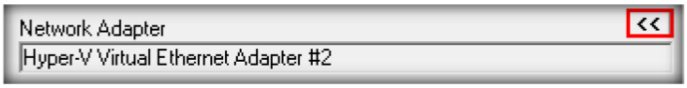


Network Connection: vEthernet (Realtek PCIe GBE Family Controller - Virtual Switch)

FIGURE 2.6: SMAC Network Connection information

SMAC does not change the hardware burned-in MAC addresses. SMAC changes the software-based MAC addresses, and the new MAC addresses you change are sustained from reboots.

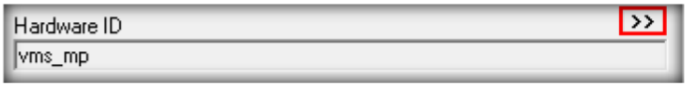
8. Clicking the backward arrow button in **Network Adapter** will again display the **Network Connection** information. These buttons allow to toggle between the Network Connection and Network Adapter information.



Network Adapter: Hyper-V Virtual Ethernet Adapter #2

FIGURE 2.7: SMAC Network Adapter information

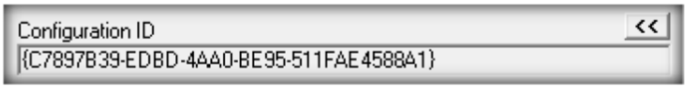
9. Similarly, the Hardware ID and Configuration ID display their respective names.
10. Click the forward arrow button in **Hardware ID** to display the **Configuration ID** information.



Hardware ID: vms_mp

FIGURE 2.8: SMAC Hardware ID display

11. Clicking the backward arrow button in **Configuration ID** will again display the **Hardware ID information**. These buttons allow to toggle between the Hardware ID and Configuration ID information.



Configuration ID: {C7897B39-EDBD-4AA0-BE95-511FAE4588A1}

FIGURE 2.9: SMAC Configuration ID display

TASK 2

Viewing IPConfig Information

12. To bring up the **ipconfig** information, click **IPConfig**.

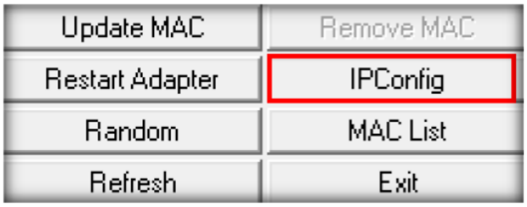
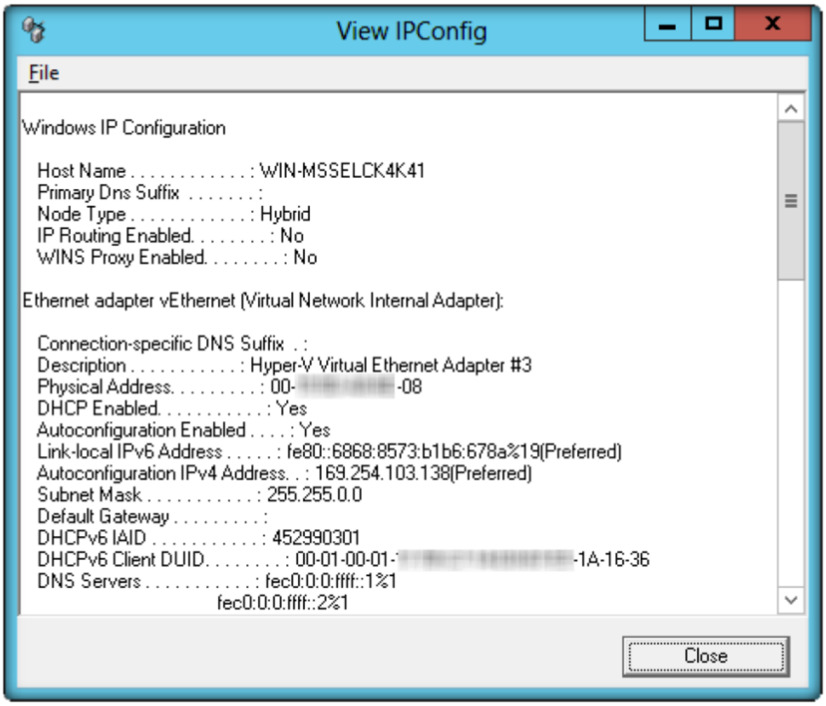

Update MAC
Remove MAC
Restart Adapter
IPConfig
Random
MAC List
Refresh
Exit

FIGURE 2.10: SMAC to view the information of IPConfig

13. The **IPConfig** window pops up, and you can also save the information by clicking the **File** menu at the top of the window.


View IPConfig
File
Close

```
Windows IP Configuration

   Host Name . . . . . . . . . . . . : WIN-MSSELCK4K41
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter vEthernet (Virtual Network Internal Adapter):

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Hyper-V Virtual Ethernet Adapter #3
   Physical Address. . . . . . . . . : 00-[redacted]-08
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::6868:8573:b1b6:678a%19(Preferred)
   Autoconfiguration IPv4 Address. . : 169.254.103.138(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 452990301
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-[redacted]-1A-16-36
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
```

The IPConfig information will show in the "View IPConfig Window. You can use the File menu to save or print the IPConfig information.

FIGURE 2.11: SMAC IPConfig information

14. You can also import the MAC address list into SMAC by clicking **MAC List**.

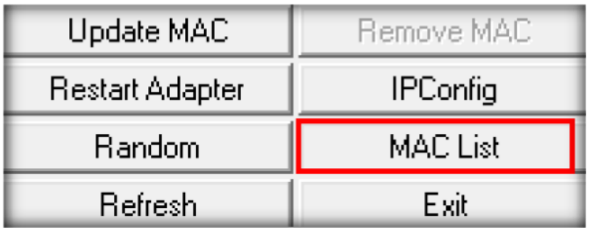

Update MAC
Remove MAC
Restart Adapter
IPConfig
Random
MAC List
Refresh
Exit

FIGURE 2.12: SMAC listing MAC addresses

15. If there is no address in the **MAC address** field, click **Load List** to select a MAC address list file you have created.

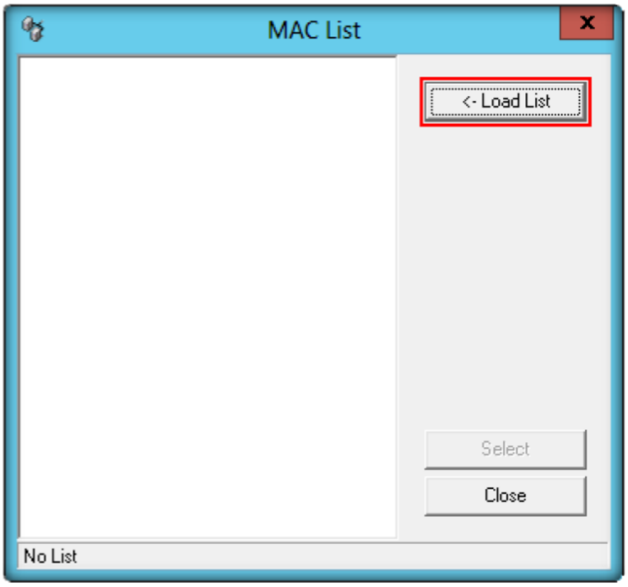

MAC List
<- Load List
Select
Close
No List

FIGURE 2.13 SMAC MAC List window

The IPConfig information will show in the "View IPConfig Window. You can use the File menu to save or print the IPConfig information.

16. Select the **Sample_MAC_Address_List.txt** file from the **Load MAC List** window.

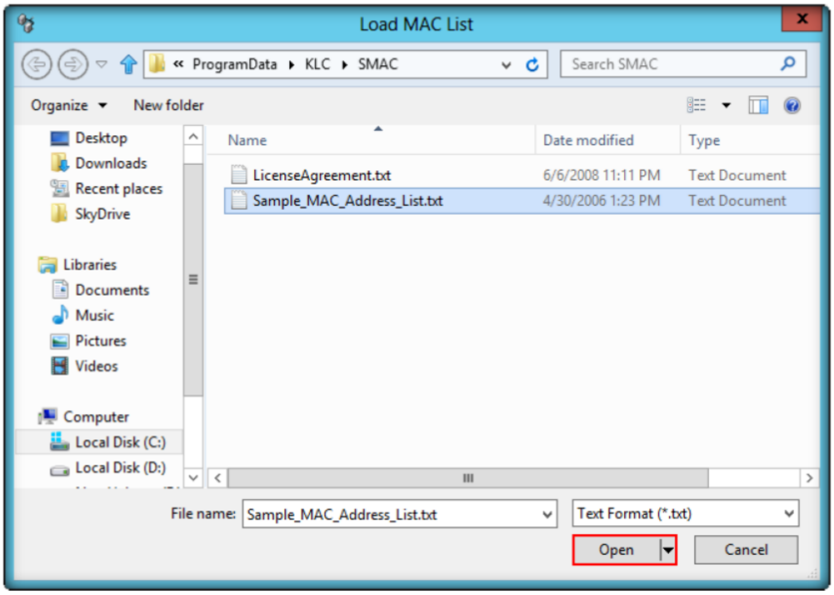
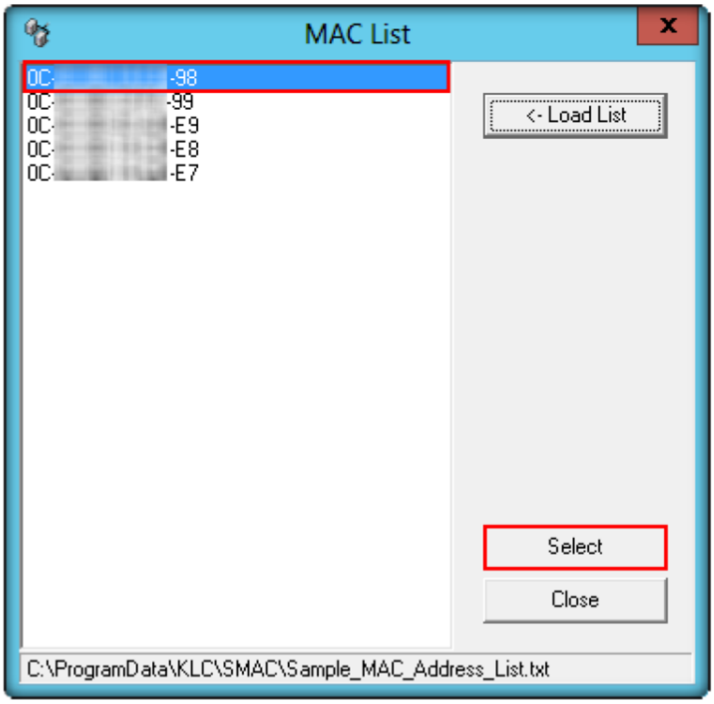

Load MAC List
« ProgramData ▸ KLC ▸ SMAC
Search SMAC
Organize
New folder
Desktop
Downloads
Recent places
SkyDrive
Libraries
Documents
Music
Pictures
Videos
Computer
Local Disk (C:)
Local Disk (D:)
Name
Date modified
Type
LicenseAgreement.txt
6/6/2008 11:11 PM
Text Document
Sample_MAC_Address_List.txt
4/30/2006 1:23 PM
Text Document
File name:
Sample_MAC_Address_List.txt
Text Format (*.txt)
Open
Cancel

FIGURE 2.14: SMAC MAC List window

When changing MAC address, you MUST assign MAC addresses according to IANA Number Assignments database. For example, "00-00-00-00-00-00" is not a valid MAC address, therefore, even though you can update this address, it may be rejected by the NIC device driver because it is not valid, and TRUE MAC address will be used instead. Otherwise, "00-00-00-00-00-00" may be accepted by the NIC device driver; however, the device will not function.

17. A list of MAC addresses will be added to the **MAC List** in SMAC. Choose a **MAC Address** and click **Select**. This MAC Address will be copied to **New Spoofed MAC Address** on the main SMAC screen.

SMAC is created and maintained by Certified Information Systems Security Professionals (CISSPs), Certified Information System Auditors (CISAs), Microsoft Certified Systems Engineers (MCSEs), and professional software engineers.



0C-[redacted]-98
0C-[redacted]-99
0C-[redacted]-E9
0C-[redacted]-E8
0C-[redacted]-E7

C:\ProgramData\KLC\SMAC\Sample_MAC_Address_List.txt

FIGURE 2.15: SMAC MAC List window

SMAC displays the following information about a Network Interface Card (NIC).

- Device ID
- Active Status
- NIC Description
- Spoofed status
- IP Address
- Active MAC address
- Spoofed MAC Address
- NIC Hardware ID
- NIC Configuration ID

18. To restart Network Adapter, click **Restart Adapter**, which restarts the selected **Network Adapter**. Restarting the adapter causes a temporary disconnection problem for your Network Adapter.

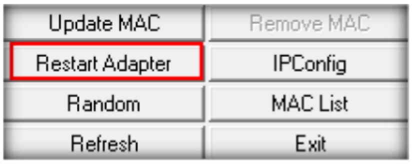


FIGURE 2.16 SMAC Restarting Network Adapter

Lab Analysis

Analyze and document the results related to the lab exercise.

Tool/Utility	Information Collected/Objectives Achieved
SMAC	▪ Host Name ▪ Node Type ▪ MAC Address ▪ IP Address ▪ DHCP Enabled ▪ Subnet Mask ▪ DNS Servers

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Evaluate and list the legitimate use of SMAC.
2. Determine whether SMAC changes hardware MAC addresses.
3. Analyze how you can remove the spoofed MAC address using the SMAC.

Internet Connection Required	
☐ **Yes**	☑ No
Platform Supported	
☑ **Classroom**	☑ iLabs

Lab

3

Sniffing a Network Using the WinArpAttacker Tool

WinArpAttacker is a program that can scan, attack, detect, and protect computers on a local area network (LAN).

ICON KEY

- 🗀 Valuable information
- ✎ Test your knowledge
- 💻 Web exercise
- 📖 Workbook review

Lab Scenario

You have already learned in the previous lab that you can conceal your identity by spoofing the MAC address. An attacker too can alter his or her MAC address and attempt to evade network intrusion detection systems, bypass access control lists, and impersonate as an authenticated user and can continue to communicate within the network when the authenticated user goes offline. Attackers can also push MAC flooding to compromise the security of network switches.

As an administrator, it is very important for you to detect odd MAC addresses on the network; you must have sound knowledge of footprinting, network protocols and their topology, TCP and UDP services, routing tables, remote access (SSH or VPN), and authentication mechanisms. You can enable port security on the switch to specify one or more MAC addresses for each port. Another way to avoid attacker sniffing on your network is by using static ARP entries. In this lab, you will learn to run the tool WinArpAttacker to sniff a network and prevent it from attacks.

Lab Objectives

The objectives of this lab are to:

- **Scan**, **Detect**, **Protect**, and **Attack** computers on local area networks (LANs):
- Scan and show the active hosts on the **LAN** within a very short time period of 2-3 seconds
- **Save** and **load** computer list files, and save the LAN regularly for a new computer list
- Update the computer list in **passive mode** using sniffing technology

- Freely **provide information** regarding the type of operating systems they employ?
- Discover the kind of **firewall**, **wireless access point** and **remote access**
- Discover any published information on the topology of the **network**
- Discover if the site is seeking help for **IT positions** that could give information regarding the network services provided by the organization
- Identify actual users and discover if they give out too much personal information, which could be used for social engineering purposes

Lab Environment

To conduct the lab you need to have:

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 08 Sniffing

- **WinArpAttacker** located at **D:\CEH-Tools\CEHv8 Module 08 Sniffing\ARP Poisoning Tools\WinArpAttacker**
- You can also download the latest version of **WinArpAttacker** from the link http://www.xfocus.net
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- A computer running **Windows Server 2012** as host machine
- **Windows 2008** running on virtual machine as target machine
- A computer updated with network devices and drivers
- Installed version of **WinPcap** drivers
- Double-click **WinArpAttacker.exe** to launch WinArpAttacker
- **Administrative** privileges to run tools

Lab Duration

Time: 10 Minutes

WinARPAttacker works on computers running Windows /2003.

Overview of Sniffing

Sniffing is performed to **collect basic information** of a target and its network. It helps to find **vulnerabilities** and to select exploits for attack. It determines network information, system information, and organizational information.

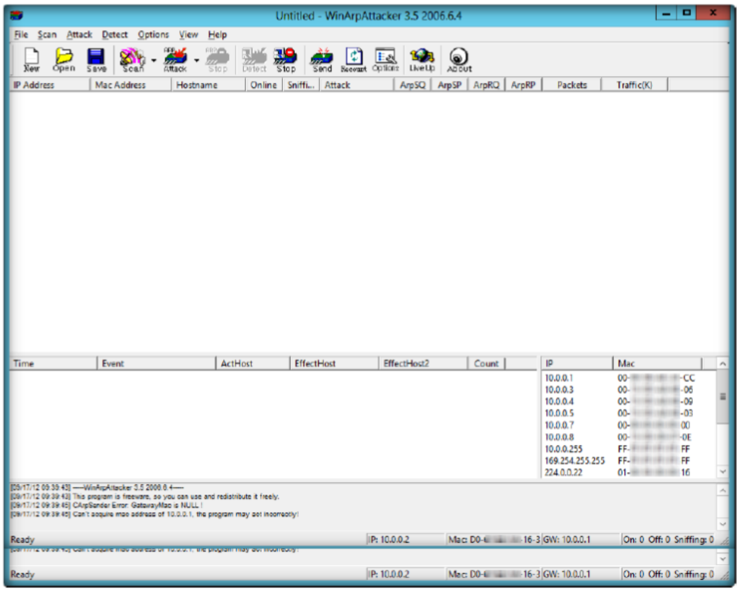
Lab Tasks

TASK 1

Scanning Hosts on the LAN

1. **Launch** Windows 8 Virtual Machine.
2. Launch **WinArpAttacker** in the host machine.

Caution:This program is dangerous, released just for research. Any possible loss caused by this program bears no relation to the author (unshadow), if you don't agree with this, you must delete it immediately.


Untitled - WinArpAttacker 3.5 2006.6.4
File Scan Attack Detect Options View Help
New Open Save Scan Attack Stop Detect Stop Send Recount Options LiveUp About
IP Address Mac Address Hostname Online Sniffi.. Attack ArpSQ ArpSP ArpRQ ArpRP Packets Traffic(K)
Time Event ActHost EffectHost EffectHost2 Count

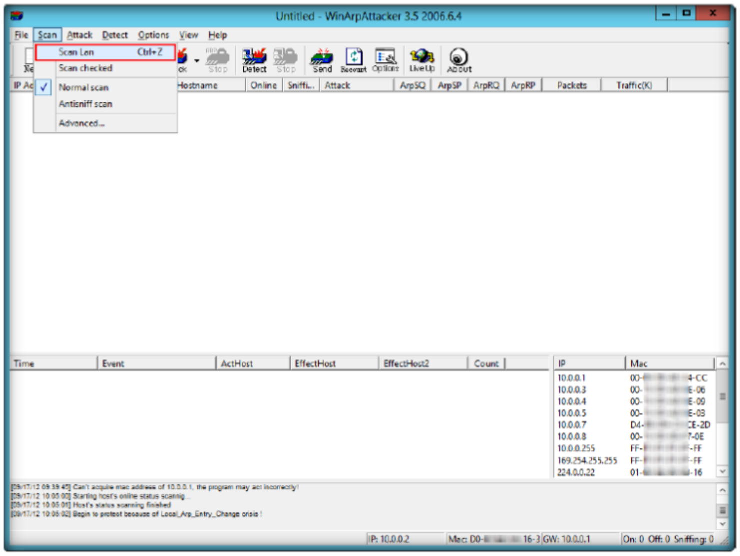
IP	Mac
10.0.0.1	00-[redacted]-CC
10.0.0.3	00-[redacted]-06
10.0.0.4	00-[redacted]-09
10.0.0.5	00-[redacted]-03
10.0.0.7	00-[redacted]00
10.0.0.8	00-[redacted]-0E
10.0.0.255	FF-[redacted]FF
169.254.255.255	FF-[redacted]FF
224.0.0.22	01-[redacted]16

```
[09/17/12 09:39:43] ——WinArpAttacker 3.5 2006.6.4——
[09/17/12 09:39:43] This program is freeware, so you can use and redistribute it freely.
[09/17/12 09:39:45] CArpSander Error: GatewayMac is NULL !
[09/17/12 09:39:45] Can't acquire mac address of 10.0.0.1, the program may act incorrectly!
Ready    IP: 10.0.0.2    Mac: D0-[redacted]-16-3  GW: 10.0.0.1    On: 0  Off: 0  Sniffing: 0
```

FIGURE 31: WinArpAttacker main window

WinArpAttacker is a program that can scan, attack, detect, and protect computers on a local area network.

3. Click the **Scan** option from the toolbar menu and select **Scan LAN**.
4. The scan shows the **active hosts** on the LAN in a very short period of time (2-3 seconds).
5. The **Scan** option has two modes: **Normal scan** and **Antisniff scan**.


Untitled - WinArpAttacker 3.5 2006.6.4
File Scan Attack Detect Options View Help
Scan Lan Ctrl+Z
Scan checked
✓ Normal scan
Antisniff scan
Advanced...
Stop Detect Stop Send Recount Options LiveUp About
Hostname Online Sniffi.. Attack ArpSQ ArpSP ArpRQ ArpRP Packets Traffic(K)
Time Event ActHost EffectHost EffectHost2 Count

IP	Mac
10.0.0.1	00-[redacted]4-CC
10.0.0.3	00-[redacted]E-06
10.0.0.4	00-[redacted]E-09
10.0.0.5	00-[redacted]E-03
10.0.0.7	D4-[redacted]CE-2D
10.0.0.8	00-[redacted]7-0E
10.0.0.255	FF-[redacted]-FF
169.254.255.255	FF-[redacted]-FF
224.0.0.22	01-[redacted]-16

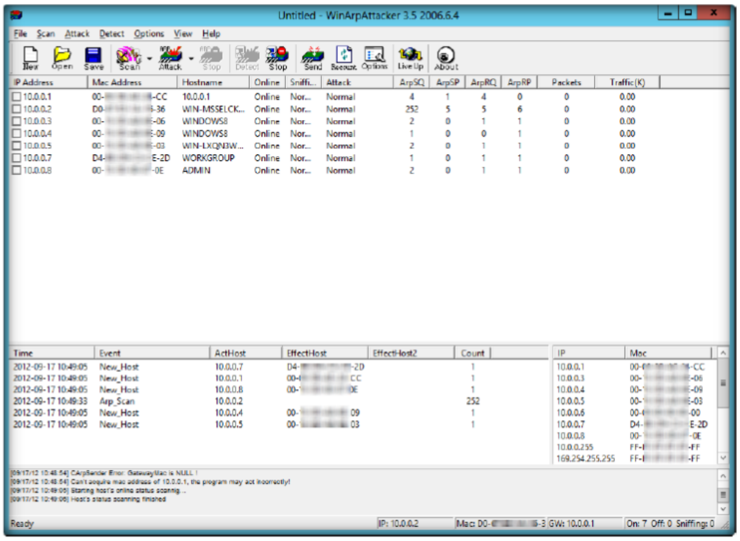
```
[09/17/12 09:39:45] Can't acquire mac address of 10.0.0.1, the program may act incorrectly!
[09/17/12 10:05:00] Starting host's online status scannig...
[09/17/12 10:05:01] Host's status scanning finished
[09/17/12 10:05:02] Begin to protect because of Local_Arp_Entry_Change crisis !
IP: 10.0.0.2    Mac: D0-[redacted]16-3  GW: 10.0.0.1    On: 0  Off: 0  Sniffing: 0
```

FIGURE 3.2: WinArpAttacker Scan options

The option scan can scan and show the active hosts on the LAN within a very short time. It has two scan modes, Normal andAntisniff. The second is to find who is sniffing on the LAN.

6. Scanning saves and loads a computer list file and also scans the LAN regularly for new computer lists.

In this tool, attacks can pull and collect all the packets on the LAN.



IP Address	Mac Address	Hostname	Online	Sniffi...	Attack	ArpSQ	ArpSP	ArpRQ	ArpRP	Packets	Traffic(K)
☐ 10.0.0.1	00-[redacted]-CC	10.0.0.1	Online	Nor...	Normal	4	1	4	0	0	0.00
☐ 10.0.0.2	D0-[redacted]-36	WIN-MSSELCK...	Online	Nor...	Normal	252	5	5	6	0	0.00
☐ 10.0.0.3	00-[redacted]E-06	WINDOWS8	Online	Nor...	Normal	2	0	1	1	0	0.00
☐ 10.0.0.4	00-[redacted]E-09	WINDOWS8	Online	Nor...	Normal	1	0	0	1	0	0.00
☐ 10.0.0.5	00-[redacted]E-03	WIN-LXQN3W...	Online	Nor...	Normal	2	0	1	1	0	0.00
☐ 10.0.0.7	D4-[redacted]E-2D	WORKGROUP	Online	Nor...	Normal	1	0	1	1	0	0.00
☐ 10.0.0.8	00-[redacted]-0E	ADMIN	Online	Nor...	Normal	2	0	1	1	0	0.00

Time	Event	ActHost	EffectHost	EffectHost2	Count
2012-09-17 10:49:05	New_Host	10.0.0.7	D4-[redacted]-2D		1
2012-09-17 10:49:05	New_Host	10.0.0.1	00-[redacted]CC		1
2012-09-17 10:49:05	New_Host	10.0.0.8	00-[redacted]0E		1
2012-09-17 10:49:33	Arp_Scan	10.0.0.2			252
2012-09-17 10:49:05	New_Host	10.0.0.4	00-[redacted]09		1
2012-09-17 10:49:05	New_Host	10.0.0.5	00-[redacted]03		1

IP	Mac
10.0.0.1	00-[redacted]-CC
10.0.0.3	00-[redacted]E-06
10.0.0.4	00-[redacted]E-09
10.0.0.5	00-[redacted]E-03
10.0.0.6	00-[redacted]-00
10.0.0.7	D4-[redacted]E-2D
10.0.0.8	00-[redacted]-0E
10.0.0.255	FF-[redacted]-FF
169.254.255.255	FF-[redacted]-FF

```
[09/17/12 10:48:54] CArpSender Error: GatewayMac is NULL !
[09/17/12 10:48:54] Can't acquire mac address of 10.0.0.1, the program may act incorrectly!
[09/17/12 10:49:05] Starting host's online status scannig...
[09/17/12 10:49:06] Host's status scanning finished
```

Ready | IP: 10.0.0.2 | Mac: D0-[redacted]-3 | GW: 10.0.0.1 | On: 7 Off: 0 Sniffing: 0

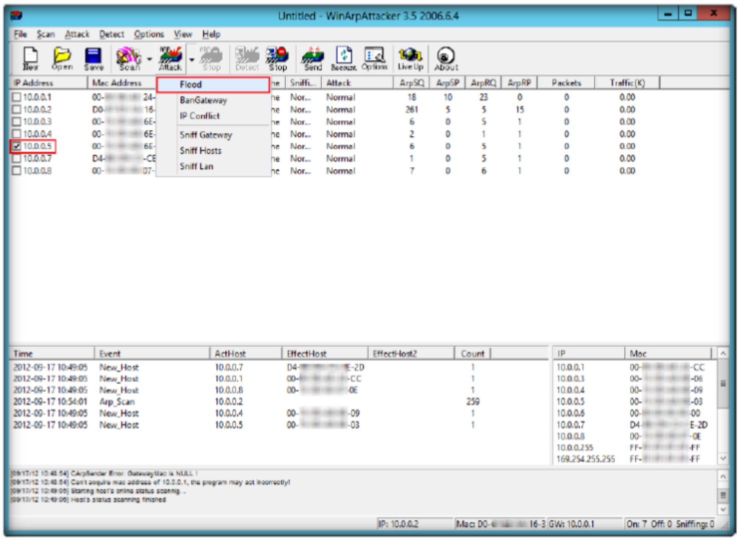
FIGURE 3.3: WinArpAttacker Loading a Computer List window

TASK 2

ARP Attack

7. By performing the attack action, scanning can pull and collect all the packets on the LAN.

8. Select a host (10.0.0.5 – Windows Server 2008) from the displayed list and select **Attack -> Flood**.



IP Address	Mac Address	ne	Sniffi...	Attack	ArpSQ	ArpSP	ArpRQ	ArpRP	Packets	Traffic(K)
☐ 10.0.0.1	00-[redacted] 24-	ne	Nor...	Normal	18	10	23	0	0	0.00
☐ 10.0.0.2	D0-[redacted] 16-	ne	Nor...	Normal	261	5	5	15	0	0.00
☐ 10.0.0.3	00-[redacted] 6E-	ne	Nor...	Normal	6	0	5	1	0	0.00
☐ 10.0.0.4	00-[redacted] 6E-	ne	Nor...	Normal	2	0	1	1	0	0.00
☑ 10.0.0.5	00-[redacted] 6E-	ne	Nor...	Normal	6	0	5	1	0	0.00
☐ 10.0.0.7	D4-[redacted]-CE	ne	Nor...	Normal	1	0	5	1	0	0.00
☐ 10.0.0.8	00-[redacted]07-	ne	Nor...	Normal	7	0	6	1	0	0.00

Time	Event	ActHost	EffectHost	EffectHost2	Count
2012-09-17 10:49:05	New_Host	10.0.0.7	D4-[redacted]E-2D		1
2012-09-17 10:49:05	New_Host	10.0.0.1	00-[redacted]-CC		1
2012-09-17 10:49:05	New_Host	10.0.0.8	00-[redacted]0E		1
2012-09-17 10:54:01	Arp_Scan	10.0.0.2			259
2012-09-17 10:49:05	New_Host	10.0.0.4	00-[redacted]-09		1
2012-09-17 10:49:05	New_Host	10.0.0.5	00-[redacted]-03		1

IP	Mac
10.0.0.1	00-[redacted]-CC
10.0.0.3	00-[redacted]-06
10.0.0.4	00-[redacted]-09
10.0.0.5	00-[redacted]-03
10.0.0.6	00-[redacted]-00
10.0.0.7	D4-[redacted]E-2D
10.0.0.8	00-[redacted]-0E
10.0.0.255	FF-[redacted]-FF
169.254.255.255	FF-[redacted]-FF

```
[09/17/12 10:48:54] CArpSender Error: GatewayMac is NULL !
[09/17/12 10:48:54] Can't acquire mac address of 10.0.0.1, the program may act incorrectly!
[09/17/12 10:49:05] Starting host's online status scannig...
[09/17/12 10:49:06] Host's status scanning finished
```

IP: 10.0.0.2 | Mac: D0-[redacted]16-3 | GW: 10.0.0.1 | On: 7 Off: 0 Sniffing: 0

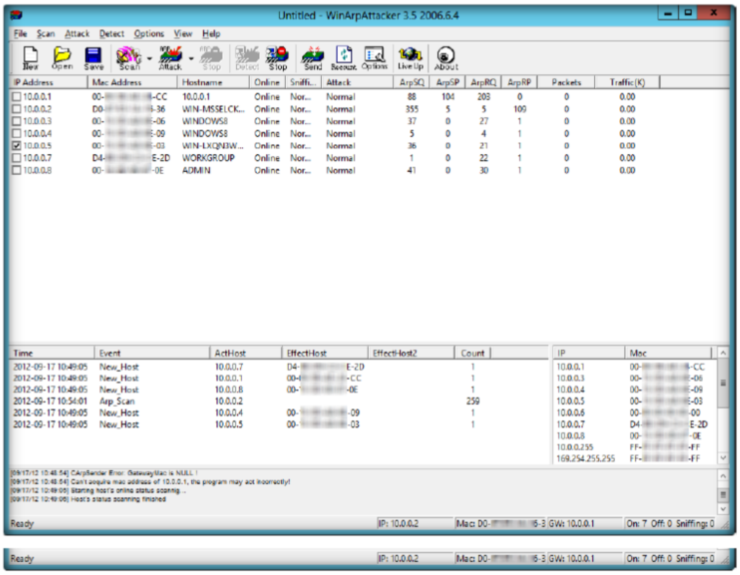
FIGURE 3.4: WinArpAttacker ARP Attack type

The Flood option sends IP conflict packets to target computers as fast as possible. If you send too many, the target computers go down.

9. Scanning acts as another gateway or IP-forwarder without other user recognition on the LAN, while spoofing ARP tables.

10. All the data sniffed by spoofing and forwarded by the WinArpAttackerIP-forward functions are counted, as shown in the main interface.

The BanGatewayoption tells the gateway wrong MAC addresses of target computers, so the targets can't receive packets from the Internet. This attack is to forbid the targets access the Internet.


Untitled - WinArpAttacker 3.5 2006.6.4
File Scan Attack Detect Options View Help
New Open Save Scan Attack Stop Detect Stop Send Recount Options Live Up About

IP Address	Mac Address	Hostname	Online	Sniffi...	Attack	ArpSQ	ArpSP	ArpRQ	ArpRP	Packets	Traffic(K)
☐ 10.0.0.1	00-[redacted]-CC	10.0.0.1	Online	Nor...	Normal	88	104	203	0	0	0.00
☐ 10.0.0.2	D0-[redacted]-36	WIN-MSSELCK...	Online	Nor...	Normal	355	5	5	109	0	0.00
☐ 10.0.0.3	00-[redacted]-06	WINDOWS8	Online	Nor...	Normal	37	0	27	1	0	0.00
☐ 10.0.0.4	00-[redacted]-09	WINDOWS8	Online	Nor...	Normal	5	0	4	1	0	0.00
☑ 10.0.0.5	00-[redacted]-03	WIN-LXQN3W...	Online	Nor...	Normal	36	0	21	1	0	0.00
☐ 10.0.0.7	D4-[redacted]E-2D	WORKGROUP	Online	Nor...	Normal	1	0	22	1	0	0.00
☐ 10.0.0.8	00-[redacted]-0E	ADMIN	Online	Nor...	Normal	41	0	30	1	0	0.00

Time	Event	ActHost	EffectHost	EffectHost2	Count
2012-09-17 10:49:05	New_Host	10.0.0.7	D4-[redacted]E-2D		1
2012-09-17 10:49:05	New_Host	10.0.0.1	00-[redacted]-CC		1
2012-09-17 10:49:05	New_Host	10.0.0.8	00-[redacted]-0E		1
2012-09-17 10:54:01	Arp_Scan	10.0.0.2			259
2012-09-17 10:49:05	New_Host	10.0.0.4	00-[redacted]-09		1
2012-09-17 10:49:05	New_Host	10.0.0.5	00-[redacted]-03		1

IP	Mac
10.0.0.1	00-[redacted]-CC
10.0.0.3	00-[redacted]-06
10.0.0.4	00-[redacted]-09
10.0.0.5	00-[redacted]-03
10.0.0.6	00-[redacted]-00
10.0.0.7	D4-[redacted]E-2D
10.0.0.8	00-[redacted]-0E
10.0.0.255	FF-[redacted]-FF
169.254.255.255	FF-[redacted]-FF

```
[09/17/12 10:48:54] CArpSender Error: GatewayMac is NULL !
[09/17/12 10:48:54] Can't acquire mac address of 10.0.0.1, the program may act incorrectly!
[09/17/12 10:49:06] Starting host's online status scannig...
[09/17/12 10:49:06] Host's status scanning finished
```

Ready | IP: 10.0.0.2 | Mac: D0-[redacted]6-3 | GW: 10.0.0.1 | On: 7 Off: 0 Sniffing: 0

Ready | IP: 10.0.0.2 | Mac: D0-[redacted]6-3 | GW: 10.0.0.1 | On: 7 Off: 0 Sniffing: 0

FIGURE 3.5: WinArpAttacker data sniffed by spoofing

The option, IPConflict, like ARP Flood, regularlysendsIP conflict packets to target computers, so that users may not be able to work because of regular ip conflict messages. In addition, the targets can't access the LAN.

11. Click **Save** to save the report.

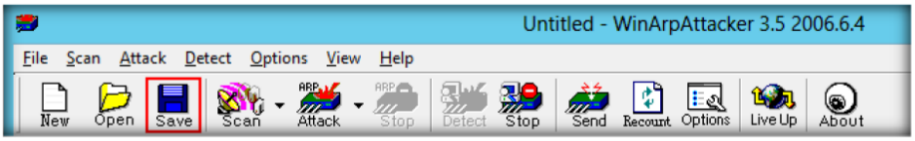

Untitled - WinArpAttacker 3.5 2006.6.4
File
Scan
Attack
Detect
Options
View
Help
New
Open
Save
Scan
Attack
Stop
Detect
Stop
Send
Recount
Options
Live Up
About

FIGURE 3.6: WinArpAttacker toolbar options

12. Select a desired location and click **Save** the save the report.

Lab Analysis

Analyze and document the scanned, attacked IP addresses discovered in the lab.

Tool/Utility	Information Collected/Objectives Achieved
WinArpAttacker	▪ Host Name ▪ Node Type ▪ MAC Address ▪ IP Address ▪ DHCP Enabled ▪ Subnet Mask ▪ DNS Servers

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. WinArp

Internet Connection Required	
☐ **Yes**	☑ No
Platform Supported	
☑ **Classroom**	☑ iLabs

Lab
4

Analyzing a Network Using the Capsa Network Analyzer

Capsa Network Analyzer is an easy-to-use Ethernet network analyzer (i.e., packet sniffer or protocol analyzer) for network monitoring and troubleshooting.

ICON KEY

- 🗀 Valuable information
- ✎ Test your knowledge
- 💻 Web exercise
- 📖 Workbook review

Lab Scenario

Using WinArpAttacker you were able to sniff the network to find information like host name, MAC address, IP address, subnet mask, DNS server, etc. An attacker, too, can use this tool to gain all such information and can set up a rogue DHCP server serving clients with false details. A DNS attack can be performed using an extension to the DNS protocol.

To prevent this, network administrators must securely configure client systems and use antivirus protection so that the attacker is unable to recruit his or her botnet army. Securely configure name servers to reduce the attacker's ability to corrupt a zone file with the amplification record. As a penetration tester you must have sound knowledge of sniffing, network protocols and their topology, TCP and UDP services, routing tables, remote access (SSH or VPN), and authentication mechanisms. This lab will teach you about using other network analyzers such as Capsa Network Analyzer to capture and analyze network traffic.

Lab Objectives

The objective of this lab is to obtain information regarding the target organization that includes, but is not limited to:

- Network traffic analysis, communication monitoring
- Network communication monitoring
- Network problem diagnosis
- Network security analysis
- Network performance detecting
- Network protocol analysis

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 08 Sniffing

Lab Environment

To carry out the lab, you need:

- **ColasoftCapsa Network Analyzer** located at **D:\CEH-Tools\CEHv8 Module 08 Sniffing\Sniffing Tools\Capsa Network Analyzer**
- You can also download the latest version of **ColasoftCapsa Network Analyzer** from the link http://www.colasoft.com
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- A computer running **Windows Server 2012** as host machine
- Windows 8 running on virtual machine as target machine
- Double-click **capsa_free_7.4.1.2626.exe** and follow the wizard-driven installation steps to install Colasoft Capsa Free Network Analyzer
- **Administrative** privileges to run tools
- A web browser with an Internet connection

Note: This lab requires an active Internet connection for license key registration

ColasoftCapsa Network Analyzer runs on Server 2003 /Server 2008/7 with 64-bit Edition.

Lab Duration

Time: 20 Minutes

Overview of Sniffing

Sniffing is performed to **collect basic information** of the target and its network. It helps to find **vulnerabilities** and select exploits for attack. It determines network information, system information, password information, and organizational information.

Sniffing can be **Active** or **Passive**.

Lab Tasks

TASK 1

Analyze Network

Capsa Network Analyzer is an easy-to-use Ethernet network analyzer (i.e., packet sniffer or protocol analyzer) for network monitoring and troubleshooting.

1. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

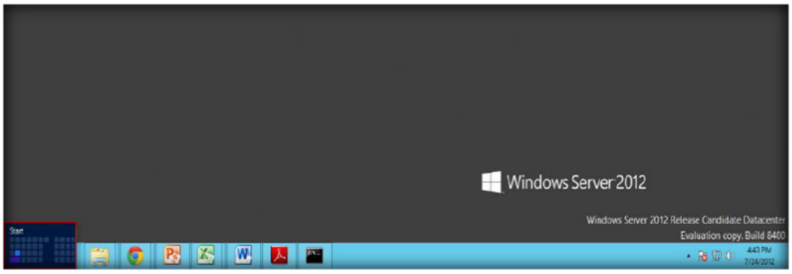

Windows Server 2012
Windows Server 2012 Release Candidate Datacenter
Evaluation copy. Build 8400
Start
4:43 PM
7/24/2012

FIGURE 4.1: Windows Server 2012 – Desktop view

2. Click **Colasoft Capsa 7 Free Network Analyzer** to launch the Network Analyzer tool.

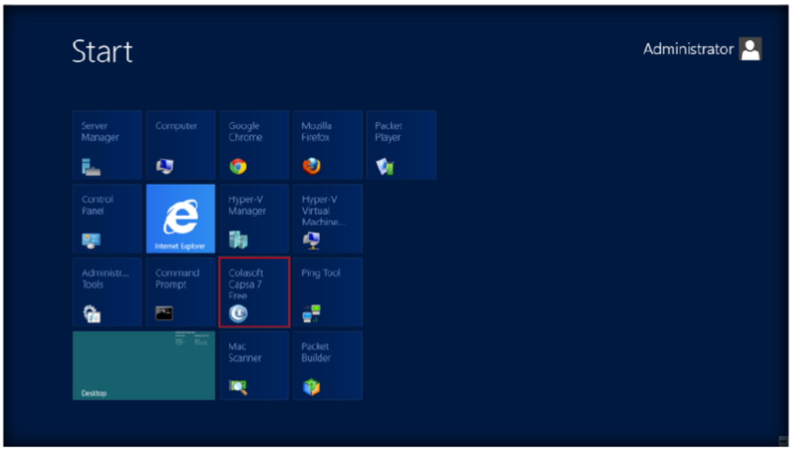
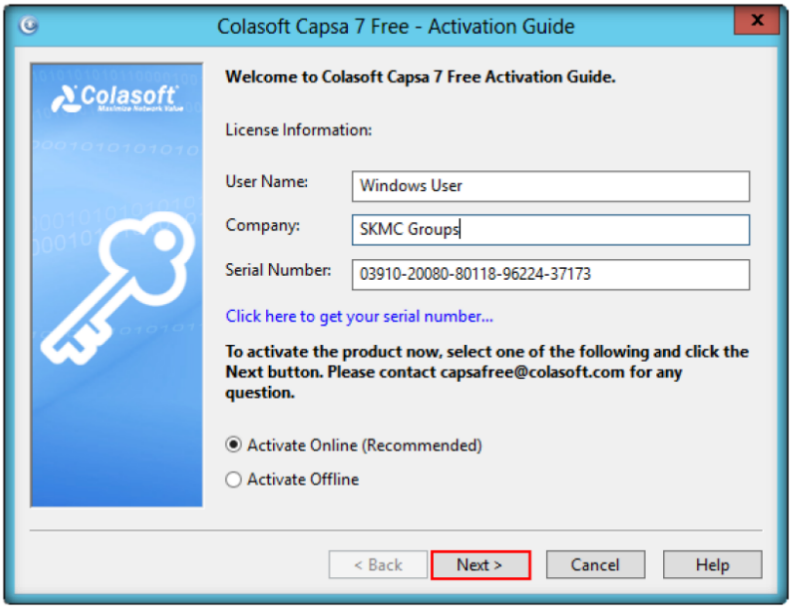

Start
Administrator
Server Manager
Computer
Google Chrome
Mozilla Firefox
Packet Player
Control Panel
Internet Explorer
Hyper-V Manager
Hyper-V Virtual Machine...
Administr... Tools
Command Prompt
Colasoft Capsa 7 Free
Ping Tool
Desktop
Mac Scanner
Packet Builder

FIGURE 4.2: Windows Server 2012 – Start menu

3. The **Colasoft Capsa 7 Free - Activation Guide** window will appear. Type the activation key that you receive in your registered email and click **Next**.


Colasoft Capsa 7 Free - Activation Guide
Colasoft

Welcome to Colasoft Capsa 7 Free Activation Guide.

License Information:

User Name: Windows User
Company: SKMC Groups
Serial Number: 03910-20080-80118-96224-37173

Click here to get your serial number...

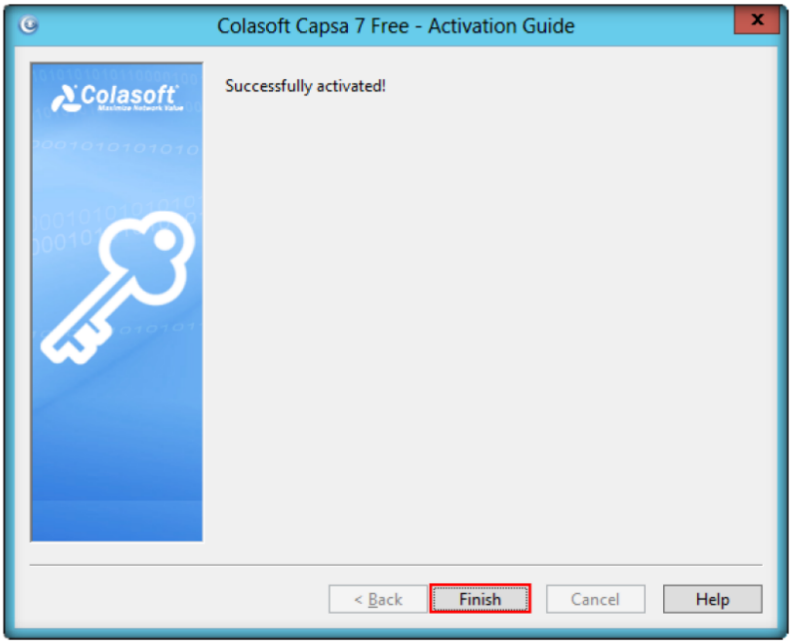
To activate the product now, select one of the following and click the Next button. Please contact capsafree@colasoft.com for any question.

● Activate Online (Recommended)
○ Activate Offline

< Back
Next >
Cancel
Help

FIGURE 4.3: Colasoft Capsa 7 Free Network Analyzer – Activation Guide window

4. Continue to click **Next** on the Activation Guide and click **Finish**.

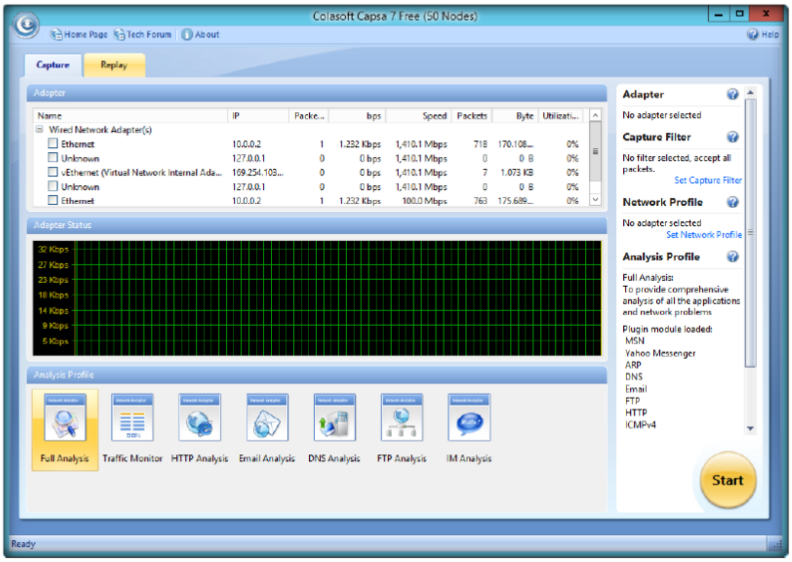


Colasoft Capsa 7 Free - Activation Guide
Colasoft
< Back
Finish
Cancel
Help

Successfully activated!

FIGURE 4.4: Colasoft Capsa 7 Free Network Analyzer – Activation successful

5. The **Colasoft Capsa 7 Free Network Analyzer** main window appears.



Colasoft Capsa 7 Free (50 Nodes)
Home Page
Tech Forum
About
Help
Capture
Replay
Adapter
Adapter Status
32 Kbps
27 Kbps
23 Kbps
18 Kbps
14 Kbps
9 Kbps
5 Kbps
Analysis Profile
Full Analysis
Traffic Monitor
HTTP Analysis
Email Analysis
DNS Analysis
FTP Analysis
IM Analysis
Start
Ready

Name	IP	Packe...	bps	Speed	Packets	Byte	Utilizati...
Wired Network Adapter(s)							
☐ Ethernet	10.0.0.2	1	1.232 Kbps	1,410.1 Mbps	718	170.108...	0%
☐ Unknown	127.0.0.1	0	0 bps	1,410.1 Mbps	0	0 B	0%
☐ vEthernet (Virtual Network Internal Ada...	169.254.103...	0	0 bps	1,410.1 Mbps	7	1.073 KB	0%
☐ Unknown	127.0.0.1	0	0 bps	1,410.1 Mbps	0	0 B	0%
☐ Ethernet	10.0.0.2	1	1.232 Kbps	100.0 Mbps	763	175.689...	0%

Adapter

No adapter selected

Capture Filter

No filter selected, accept all packets.

Set Capture Filter

Network Profile

No adapter selected

Set Network Profile

Analysis Profile

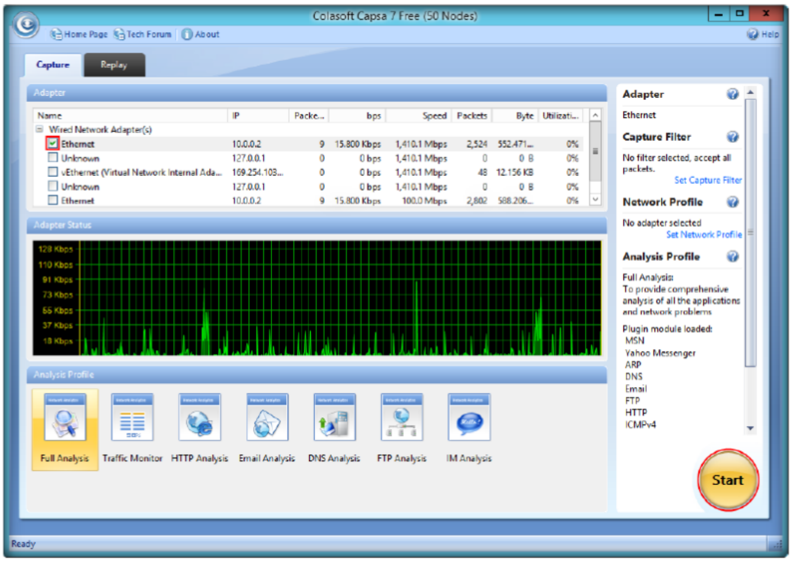
Full Analysis:
To provide comprehensive analysis of all the applications and network problems

Plugin module loaded:
MSN
Yahoo Messenger
ARP
DNS
Email
FTP
HTTP
ICMPv4

FIGURE 4.5: Colasoft Capsa Network Analyzer main screen

As a network analyzer, Capsa make it easy to monitor and analyze network traffic with its intuitive and information-rich tab views.

6. In the **Capture** tab of the main window, select the **Ethernet** check box in **Adapter** and click **Start** to create a new project.


Colasoft Capsa 7 Free (50 Nodes)
Home Page
Tech Forum
About
Help
Capture
Replay
Adapter
Adapter Status
128 Kbps
110 Kbps
91 Kbps
73 Kbps
55 Kbps
37 Kbps
18 Kbps
Analysis Profile
Full Analysis
Traffic Monitor
HTTP Analysis
Email Analysis
DNS Analysis
FTP Analysis
IM Analysis
Start
Ready

Name	IP	Packe...	bps	Speed	Packets	Byte	Utilizati...
⊟ Wired Network Adapter(s)							
☑ Ethernet	10.0.0.2	9	15.800 Kbps	1,410.1 Mbps	2,524	552.471...	0%
☐ Unknown	127.0.0.1	0	0 bps	1,410.1 Mbps	0	0 B	0%
☐ vEthernet (Virtual Network Internal Ada...	169.254.103...	0	0 bps	1,410.1 Mbps	48	12.156 KB	0%
☐ Unknown	127.0.0.1	0	0 bps	1,410.1 Mbps	0	0 B	0%
☐ Ethernet	10.0.0.2	9	15.800 Kbps	100.0 Mbps	2,802	588.206...	0%

Adapter
Ethernet

Capture Filter
No filter selected, accept all packets.
Set Capture Filter

Network Profile
No adapter selected
Set Network Profile

Analysis Profile
Full Analysis:
To provide comprehensive analysis of all the applications and network problems

Plugin module loaded:
MSN
Yahoo Messenger
ARP
DNS
Email
FTP
HTTP
ICMPv4

FIGURE 4.6: Colasoft Capsa Network Analyzer creating a New Project

7. **Dashboard** provides various graphs and charts of the statistics. You can view the analysis report in a graphical format in the **Dashboard** section of **Node Explorer**.

The network utilization rate is the ratio of current network traffic to the maximum traffic that a port can handle. It indicates the bandwidth use in the network.

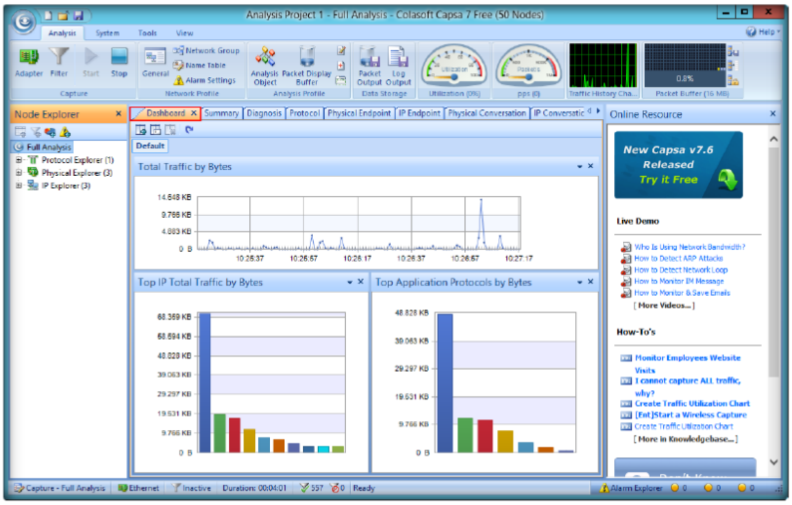
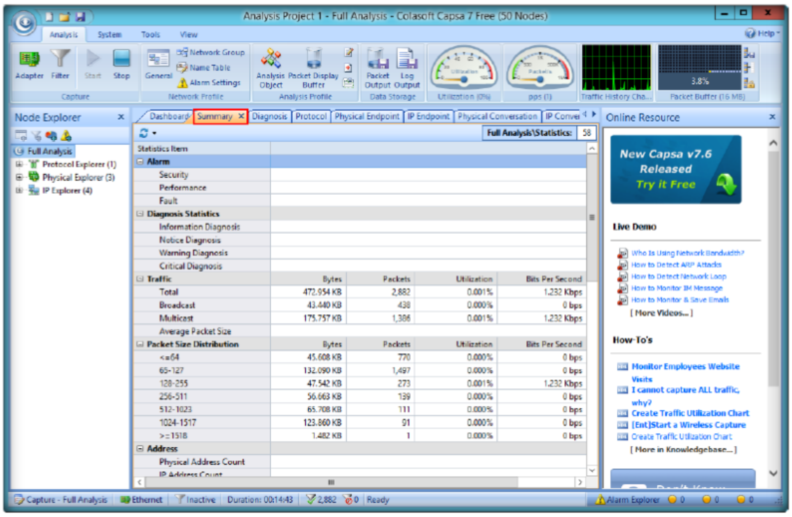

Analysis Project 1 - Full Analysis - Colasoft Capsa 7 Free (50 Nodes)
Analysis
System
Tools
View
Help
Adapter
Filter
Start
Stop
Capture
General
Network Group
Name Table
Alarm Settings
Network Profile
Analysis Object
Packet Display Buffer
Analysis Profile
Packet Output
Log Output
Data Storage
Utilization (0%)
pps (0)
Traffic History Cha...
Packet Buffer (16 MB)
0.8%
Node Explorer
Full Analysis
Protocol Explorer (1)
Physical Explorer (3)
IP Explorer (3)
Dashboard
Summary
Diagnosis
Protocol
Physical Endpoint
IP Endpoint
Physical Conversation
IP Conversatic
Default
Total Traffic by Bytes
14.648 KB
9.766 KB
4.883 KB
0 B
10:25:37
10:26:57
10:26:17
10:26:37
10:26:57
10:27:17
Top IP Total Traffic by Bytes
68.359 KB
58.594 KB
48.828 KB
39.063 KB
29.297 KB
19.531 KB
9.766 KB
0 B
Top Application Protocols by Bytes
48.828 KB
39.063 KB
29.297 KB
19.531 KB
9.766 KB
0 B
Online Resource
New Capsa v7.6 Released Try it Free
Live Demo
Who Is Using Network Bandwidth?
How to Detect ARP Attacks
How to Detect Network Loop
How to Monitor IM Message
How to Monitor & Save Emails
[More Videos...]
How-To's
Monitor Employees Website Visits
I cannot capture ALL traffic, why?
Create Traffic Utilization Chart
[Ent]Start a Wireless Capture
Create Traffic Utilization Chart
[More in Knowledgebase...]
Capture - Full Analysis
Ethernet
Inactive
Duration: 00:04:01
557
0
Ready
Alarm Explorer
0
0
0

FIGURE 4.7: Colasoft Capsa Network Analyzer Dashboard

8. The **Summary** tab provides full general analysis and statistical information of the selected node in the **Node Explorer** window.


Analysis Project 1 - Full Analysis - Colasoft Capsa 7 Free (50 Nodes)
Analysis
System
Tools
View
Adapter
Filter
Start
Stop
General
Network Group
Name Table
Alarm Settings
Analysis Object
Packet Display Buffer
Packet Output
Log Output
Node Explorer
Full Analysis
Protocol Explorer (1)
Physical Explorer (3)
IP Explorer (4)
Dashboard
Summary
Diagnosis
Protocol
Physical Endpoint
IP Endpoint
Physical Conversation
IP Conver
Online Resource
New Capsa v7.6 Released Try it Free
Live Demo
How-To's
Capture - Full Analysis
Ethernet
Inactive
Duration: 00:14:43
2,882
0
Ready
Alarm Explorer

Full Analysis\Statistics: 58

Statistics Item	Bytes	Packets	Utilization	Bits Per Second
Alarm				
Security				
Performance				
Fault				
Diagnosis Statistics				
Information Diagnosis				
Notice Diagnosis				
Warning Diagnosis				
Critical Diagnosis				
Traffic	Bytes	Packets	Utilization	Bits Per Second
Total	472.954 KB	2,882	0.001%	1.232 Kbps
Broadcast	43.440 KB	438	0.000%	0 bps
Multicast	175.757 KB	1,386	0.001%	1.232 Kbps
Average Packet Size				
Packet Size Distribution	Bytes	Packets	Utilization	Bits Per Second
<=64	45.608 KB	770	0.000%	0 bps
65-127	132.090 KB	1,497	0.000%	0 bps
128-255	47.542 KB	273	0.001%	1.232 Kbps
256-511	56.663 KB	139	0.000%	0 bps
512-1023	65.708 KB	111	0.000%	0 bps
1024-1517	123.860 KB	91	0.000%	0 bps
>=1518	1.482 KB	1	0.000%	0 bps
Address				
Physical Address Count				
IP Address Count				

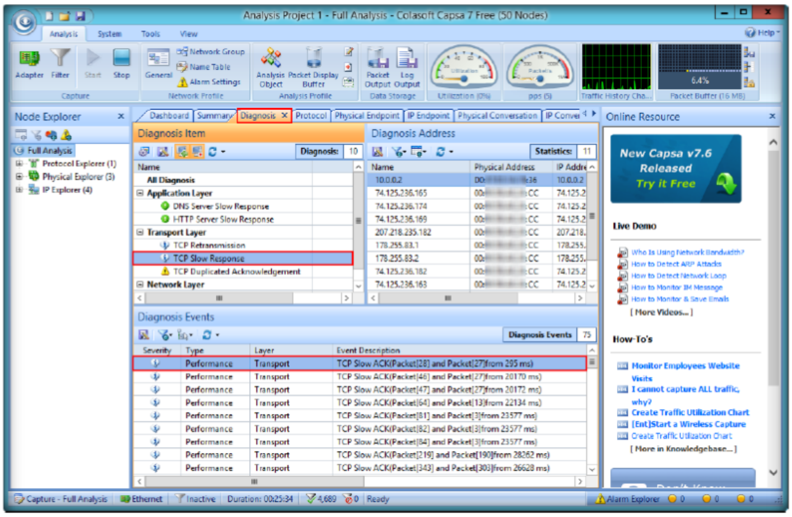
FIGURE 4.8: Colasoft Capsa Network Analyzer Summary

A high network utilization rate indicates the network is busy, whereas a low utilization rate indicates the network is idle.

9. The **Diagnosis** tab provides the real-time diagnosis events of the global network by groups of protocol layers or security levels. With this tab you can view the performance of the protocols

10. To view the slow response of TCP, click **TCP Slow Response** in **Transport Layer**, which in turn will highlight the slowest response in **Diagnosis Events**.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 08 Sniffing


Analysis Project 1 - Full Analysis - Colasoft Capsa 7 Free (50 Nodes)
Analysis
System
Tools
View
Adapter
Filter
Start
Stop
General
Network Group
Name Table
Alarm Settings
Analysis Object
Packet Display Buffer
Packet Output
Log Output
Node Explorer
Full Analysis
Protocol Explorer (1)
Physical Explorer (3)
IP Explorer (4)
Dashboard
Summary
Diagnosis
Protocol
Physical Endpoint
IP Endpoint
Physical Conversation
IP Conver
Online Resource
New Capsa v7.6 Released Try it Free
Live Demo
How-To's
Capture - Full Analysis
Ethernet
Inactive
Duration: 00:25:34
4,689
0
Ready
Alarm Explorer

Diagnosis Item — Diagnosis: 10

Name
All Diagnosis
Application Layer
DNS Server Slow Response
HTTP Server Slow Response
Transport Layer
TCP Retransmission
TCP Slow Response
TCP Duplicated Acknowledgement
Network Layer

Diagnosis Address — Statistics: 11

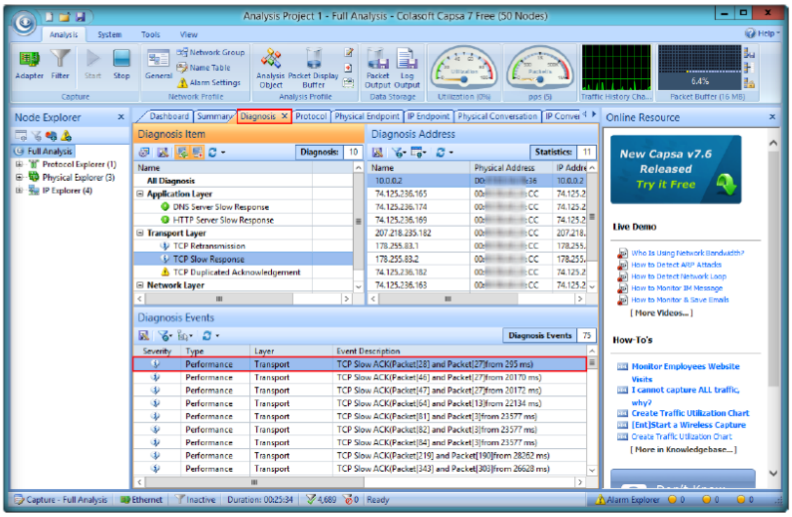
Name	Physical Address	IP Addre
10.0.0.2	[redacted]	10.0.0.2
74.125.236.165	[redacted]	74.125.2
74.125.236.174	[redacted]	74.125.2
74.125.236.169	[redacted]	74.125.2
207.218.235.182	[redacted]	207.218.
178.255.83.1	[redacted]	178.255.
178.255.83.2	[redacted]	178.255.
74.125.236.182	[redacted]	74.125.2
74.125.236.163	[redacted]	74.125.2

Diagnosis Events — Diagnosis Events: 75

Severity	Type	Layer	Event Description
	Performance	Transport	TCP Slow ACK(Packet[28] and Packet[27]from 295 ms)
	Performance	Transport	TCP Slow ACK(Packet[46] and Packet[27]from 20170 ms)
	Performance	Transport	TCP Slow ACK(Packet[47] and Packet[27]from 20172 ms)
	Performance	Transport	TCP Slow ACK(Packet[64] and Packet[13]from 22134 ms)
	Performance	Transport	TCP Slow ACK(Packet[81] and Packet[3]from 23577 ms)
	Performance	Transport	TCP Slow ACK(Packet[82] and Packet[3]from 23577 ms)
	Performance	Transport	TCP Slow ACK(Packet[84] and Packet[3]from 23577 ms)
	Performance	Transport	TCP Slow ACK(Packet[219] and Packet[190]from 28262 ms)
	Performance	Transport	TCP Slow ACK(Packet[343] and Packet[303]from 26628 ms)

FIGURE 4.9: Colasoft Capsa Network Analyzer Diagnoses

11. Double-click the highlighted **Diagnosis Event** to view the detailed information of this event.

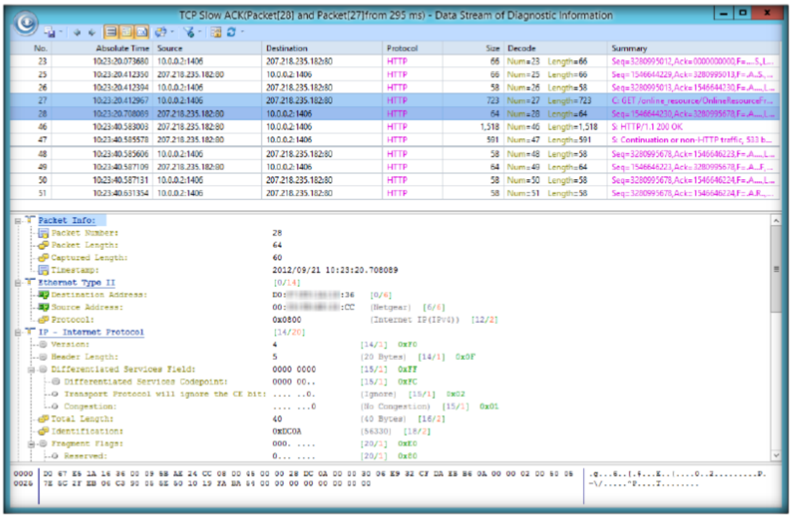


Severity	Type	Layer	Event Description
	Performance	Transport	TCP Slow ACK(Packet[28] and Packet[27]from 295 ms)
	Performance	Transport	TCP Slow ACK(Packet[46] and Packet[27]from 20170 ms)
	Performance	Transport	TCP Slow ACK(Packet[47] and Packet[27]from 20172 ms)
	Performance	Transport	TCP Slow ACK(Packet[64] and Packet[13]from 22134 ms)
	Performance	Transport	TCP Slow ACK(Packet[81] and Packet[3]from 23577 ms)
	Performance	Transport	TCP Slow ACK(Packet[82] and Packet[3]from 23577 ms)
	Performance	Transport	TCP Slow ACK(Packet[84] and Packet[3]from 23577 ms)
	Performance	Transport	TCP Slow ACK(Packet[219] and Packet[190]from 28262 ms)
	Performance	Transport	TCP Slow ACK(Packet[343] and Packet[303]from 26628 ms)

Analysis Project 1 - Full Analysis - Colasoft Capsa 7 Free (50 Nodes)
Node Explorer
Full Analysis
Protocol Explorer (1)
Physical Explorer (3)
IP Explorer (4)
Dashboard
Summary
Diagnosis
Protocol
Physical Endpoint
IP Endpoint
Physical Conversation
Diagnosis Item
All Diagnosis
Application Layer
DNS Server Slow Response
HTTP Server Slow Response
Transport Layer
TCP Retransmission
TCP Slow Response
TCP Duplicated Acknowledgement
Network Layer
Diagnosis Address
Diagnosis Events 75
Online Resource
New Capsa v7.6 Released Try it Free
Live Demo
How-To's
Capture - Full Analysis
Ethernet
Inactive
Duration: 00:25:34
4,689
Ready

FIGURE 4.10: Analyzing Diagnosis Event

12. The **TCP Slow ACK – Data Stream of Diagnostic Information** window appears, displaying Absolute Time, Source, Destination, Packet Info, TCP, IP, and other information.



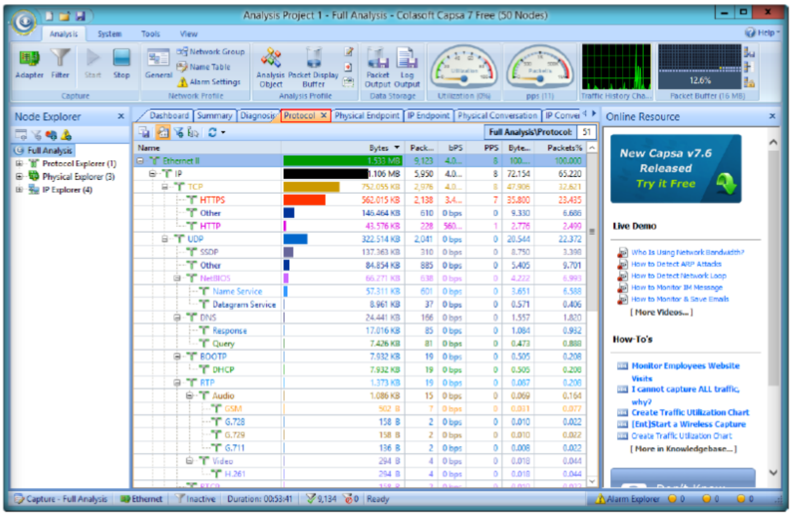
TCP Slow ACK(Packet[28] and Packet[27]from 295 ms) - Data Stream of Diagnostic Information

No.	Absolute Time	Source	Destination	Protocol	Size	Decode	Summary
23	10:23:20.073680	10.0.0.2:1406	207.218.235.182:80	HTTP	66	Num=23 Length=66	Seq=3280995012,Ack=000000000,F=....S.,L...
25	10:23:20.412350	207.218.235.182:80	10.0.0.2: 1406	HTTP	66	Num=25 Length=66	Seq= 1546644229,Ack= 3280995013,F=.A..S., ...
26	10:23:20.412394	10.0.0.2:1406	207.218.235.182:80	HTTP	58	Num=26 Length=58	Seq=3280995013,Ack= 1546644230,F=.A....,L...
27	10:23:20.412967	10.0.0.2:1406	207.218.235.182:80	HTTP	723	Num=27 Length=723	C: GET /online_resource/OnlineResourceFr...
28	10:23:20.708089	207.218.235.182:80	10.0.0.2: 1406	HTTP	64	Num=28 Length=64	Seq= 1546644230,Ack= 3280995678,F=.A....,L...
46	10:23:40.583003	207.218.235.182:80	10.0.0.2: 1406	HTTP	1,518	Num=46 Length=1,518	S: HTTP/1.1 200 OK
47	10:23:40.585578	207.218.235.182:80	10.0.0.2: 1406	HTTP	591	Num=47 Length=591	S: Continuation or non-HTTP traffic, 533 b...
48	10:23:40.585606	10.0.0.2:1406	207.218.235.182:80	HTTP	58	Num=48 Length=58	Seq=3280995678,Ack= 1546646223,F=.A....,L...
49	10:23:40.587109	207.218.235.182:80	10.0.0.2: 1406	HTTP	64	Num=49 Length=64	Seq= 1546646223,Ack= 3280995678,F=.A...F, ...
50	10:23:40.587131	10.0.0.2:1406	207.218.235.182:80	HTTP	58	Num=50 Length=58	Seq=3280995678,Ack= 1546646224,F=.A....,L...
51	10:23:40.631354	10.0.0.2:1406	207.218.235.182:80	HTTP	58	Num=51 Length=58	Seq=3280995678,Ack= 1546646224,F=.A.R..,...

```
Packet Info:
    Packet Number:                                28
    Packet Length:                                64
    Captured Length:                              60
    Timestamp:                                    2012/09/21 10:23:20.708089
Ethernet Type II                                  [0/14]
    Destination Address:                          D0:[redacted]:36      [0/6]
    Source Address:                               00:[redacted]:CC      (Netgear)  [6/6]
    Protocol:                                     0x0800                (Internet IP(IPv4))  [12/2]
IP - Internet Protocol                            [14/20]
    Version:                                      4                     [14/1]  0xF0
    Header Length:                                5                     (20 Bytes)  [14/1]  0x0F
    Differentiated Services Field:                0000 0000             [15/1]  0xFF
        Differentiated Services Codepoint:        0000 00..             [15/1]  0xFC
        Transport Protocol will ignore the CE bit: .... ..0.            (Ignore)  [15/1]  0x02
        Congestion:                               .... ...0             (No Congestion)  [15/1]  0x01
    Total Length:                                 40                    (40 Bytes)  [16/2]
    Identification:                               0xDC0A                (56330)  [18/2]
    Fragment Flags:                               000. ....             [20/1]  0xE0
        Reserved:                                 0... ....             [20/1]  0x80
```

FIGURE 4.11: TCP Slow ACK – Data Stream of Diagnostic Information window

13. The **Protocol** tab lists statistics of all protocols used in network transactions hierarchically, allowing you to view and analyze the protocols.

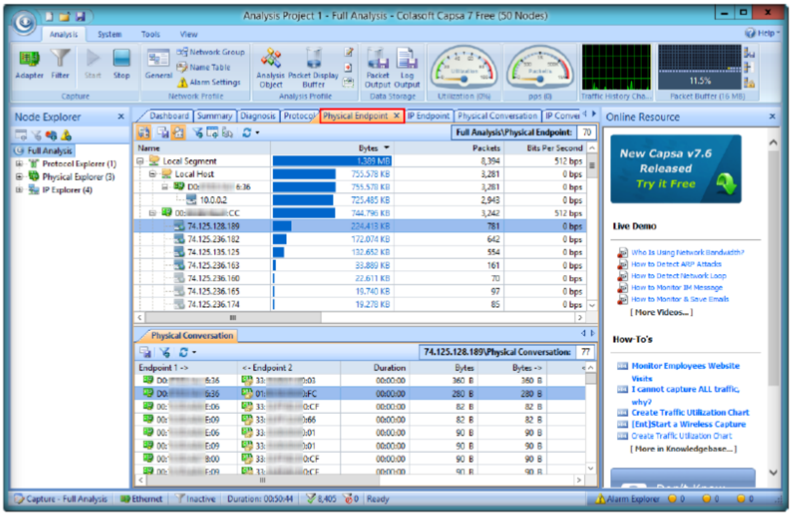

Analysis Project 1 - Full Analysis - Colasoft Capsa 7 Free (50 Nodes)
Analysis
System
Tools
View
Help
Adapter
Filter
Start
Stop
Capture
General
Network Group
Name Table
Alarm Settings
Network Profile
Analysis Object
Packet Display Buffer
Analysis Profile
Packet Output
Log Output
Data Storage
Utilization (0%)
pps (11)
Traffic History Cha...
12.6%
Packet Buffer (16 MB)
Node Explorer
Full Analysis
Protocol Explorer (1)
Physical Explorer (3)
IP Explorer (4)
Dashboard
Summary
Diagnosis
Protocol
Physical Endpoint
IP Endpoint
Physical Conversation
IP Conver
Online Resource
New Capsa v7.6 Released
Try it Free
Live Demo
Who Is Using Network Bandwidth?
How to Detect ARP Attacks
How to Detect Network Loop
How to Monitor IM Message
How to Monitor & Save Emails
[More Videos...]
How-To's
Monitor Employees Website Visits
I cannot capture ALL traffic, why?
Create Traffic Utilization Chart
[Ent]Start a Wireless Capture
Create Traffic Utilization Chart
[More in Knowledgebase...]
Capture - Full Analysis
Ethernet
Inactive
Duration: 00:53:41
9,134
0
Ready
Alarm Explorer

Full Analysis\Protocol: 51

Name	Bytes	Pack...	bPS	PPS	Byte...	Packets%
Ethernet II	1.533 MB	9,123	4.0...	8	100....	100.000
IP	1.106 MB	5,950	4.0...	8	72.154	65.220
TCP	752.055 KB	2,976	4.0...	8	47.906	32.621
HTTPS	562.015 KB	2,138	3.4...	7	35.800	23.435
Other	146.464 KB	610	0 bps	0	9.330	6.686
HTTP	43.576 KB	228	560...	1	2.776	2.499
UDP	322.514 KB	2,041	0 bps	0	20.544	22.372
SSDP	137.363 KB	310	0 bps	0	8.750	3.398
Other	84.854 KB	885	0 bps	0	5.405	9.701
NetBIOS	66.271 KB	638	0 bps	0	4.222	6.993
Name Service	57.311 KB	601	0 bps	0	3.651	6.588
Datagram Service	8.961 KB	37	0 bps	0	0.571	0.406
DNS	24.441 KB	166	0 bps	0	1.557	1.820
Response	17.016 KB	85	0 bps	0	1.084	0.932
Query	7.426 KB	81	0 bps	0	0.473	0.888
BOOTP	7.932 KB	19	0 bps	0	0.505	0.208
DHCP	7.932 KB	19	0 bps	0	0.505	0.208
RTP	1.373 KB	19	0 bps	0	0.087	0.208
Audio	1.086 KB	15	0 bps	0	0.069	0.164
GSM	502 B	7	0 bps	0	0.031	0.077
G.728	158 B	2	0 bps	0	0.010	0.022
G.729	158 B	2	0 bps	0	0.010	0.022
G.711	136 B	2	0 bps	0	0.008	0.022
Video	294 B	4	0 bps	0	0.018	0.044
H.261	294 B	4	0 bps	0	0.018	0.044

FIGURE 4.12: Colasoft Capsa Network Analyzer Protocol analysis

14. The **Physical Endpoint** tab lists statistics of all MAC addresses that communicate in the network hierarchically.


Analysis Project 1 - Full Analysis - Colasoft Capsa 7 Free (50 Nodes)
Analysis
System
Tools
View
Help
Adapter
Filter
Start
Stop
Capture
General
Network Group
Name Table
Alarm Settings
Network Profile
Analysis Object
Packet Display Buffer
Analysis Profile
Packet Output
Log Output
Data Storage
Utilization (0%)
pps (0)
Traffic History Cha...
11.5%
Packet Buffer (16 MB)
Node Explorer
Full Analysis
Protocol Explorer (1)
Physical Explorer (3)
IP Explorer (4)
Dashboard
Summary
Diagnosis
Protocol
Physical Endpoint
IP Endpoint
Physical Conversation
IP Conver
Online Resource
New Capsa v7.6 Released
Try it Free
Live Demo
Who Is Using Network Bandwidth?
How to Detect ARP Attacks
How to Detect Network Loop
How to Monitor IM Message
How to Monitor & Save Emails
[More Videos...]
How-To's
Monitor Employees Website Visits
I cannot capture ALL traffic, why?
Create Traffic Utilization Chart
[Ent]Start a Wireless Capture
Create Traffic Utilization Chart
[More in Knowledgebase...]
Physical Conversation
Capture - Full Analysis
Ethernet
Inactive
Duration: 00:50:44
8,405
0
Ready
Alarm Explorer

Full Analysis\Physical Endpoint: 70

Name	Bytes	Packets	Bits Per Second
Local Segment	1.389 MB	8,394	512 bps
Local Host	755.578 KB	3,281	0 bps
D0:[redacted]6:36	755.578 KB	3,281	0 bps
10.0.0.2	725.485 KB	2,943	0 bps
00:[redacted]:CC	744.796 KB	3,242	512 bps
74.125.128.189	224.413 KB	781	0 bps
74.125.236.182	172.074 KB	642	0 bps
74.125.135.125	132.652 KB	554	0 bps
74.125.236.163	33.889 KB	161	0 bps
74.125.236.160	22.611 KB	70	0 bps
74.125.236.165	19.740 KB	97	0 bps
74.125.236.174	19.278 KB	85	0 bps

74.125.128.189\Physical Conversation: 77

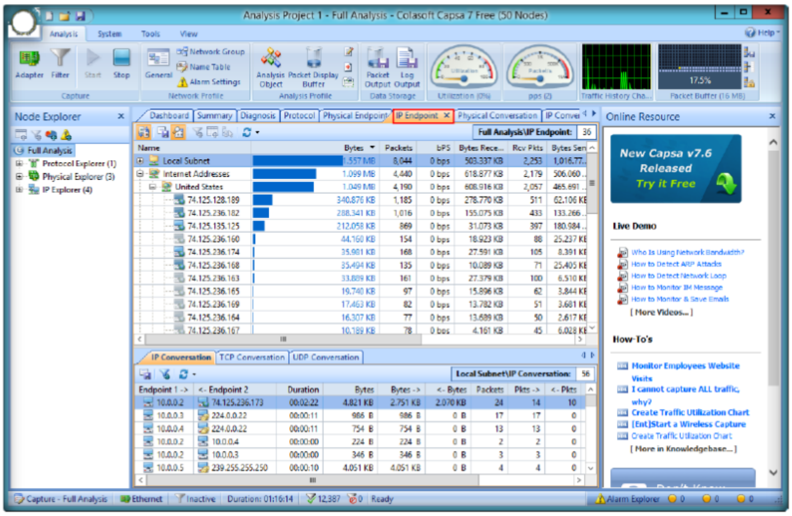
Endpoint 1 ->	<- Endpoint 2	Duration	Bytes	Bytes ->
D0:[redacted]6:36	33:[redacted]0:03	00:00:00	360 B	360 B
D0:[redacted]6:36	01:[redacted]:FC	00:00:00	280 B	280 B
00:[redacted]E:06	33:[redacted]0:CF	00:00:00	82 B	82 B
00:[redacted]E:09	33:[redacted]:66	00:00:00	82 B	82 B
00:[redacted]E:06	33:[redacted]0:01	00:00:00	90 B	90 B
00:[redacted]E:09	33:[redacted]0:01	00:00:00	90 B	90 B
00:[redacted]8:00	33:[redacted]0:CF	00:00:00	90 B	90 B

FIGURE 4.13: Colasoft Capsa Network Analyzer Physical Endpoint analysis

15. The **IP Endpoint** tab displays statistics of all IP addresses communicating within the network.

16. On the **IP Endpoint** tab, you can easily find the nodes with the highest traffic volumes, and check if there is a multicast storm or broadcast storm in your network.

As a delicate work, network analysis always requires us to view the original packets and analyze them. However, not all the network failures can be found in a very short period. Sometimes network analysis requires a long period of monitoring and must be based on the baseline of the normal network.


Analysis Project 1 - Full Analysis - Colasoft Capsa 7 Free (50 Nodes)
Analysis
System
Tools
View
Adapter
Filter
Start
Stop
General
Network Group
Name Table
Alarm Settings
Analysis Object
Packet Display Buffer
Packet Output
Log Output
Network Profile
Analysis Profile
Data Storage
Node Explorer
Dashboard
Summary
Diagnosis
Protocol
Physical Endpoint
IP Endpoint
Physical Conversation
IP Conver
Online Resource
IP Conversation
TCP Conversation
UDP Conversation

Full Analysis\IP Endpoint: 36

Name	Bytes	Packets	bPS	Bytes Rece...	Rcv Pkts	Bytes Sen
Local Subnet	1.557 MB	8,044	0 bps	503.337 KB	2,253	1,016.77...
Internet Addresses	1.099 MB	4,440	0 bps	618.877 KB	2,179	506.060...
United States	1.049 MB	4,190	0 bps	608.916 KB	2,057	465.691...
74.125.128.189	340.876 KB	1,185	0 bps	278.770 KB	511	62.106 KE
74.125.236.182	288.341 KB	1,016	0 bps	155.075 KB	433	133.266...
74.125.135.125	212.058 KB	869	0 bps	31.073 KB	397	180.984...
74.125.236.160	44.160 KB	154	0 bps	18.923 KB	88	25.237 KE
74.125.236.174	35.981 KB	168	0 bps	27.591 KB	105	8.391 KE
74.125.236.168	35.494 KB	135	0 bps	10.089 KB	71	25.405 KE
74.125.236.163	33.889 KB	161	0 bps	27.379 KB	100	6.510 KE
74.125.236.165	19.740 KB	97	0 bps	15.896 KB	62	3.844 KE
74.125.236.169	17.463 KB	82	0 bps	13.782 KB	51	3.681 KE
74.125.236.164	16.307 KB	77	0 bps	13.689 KB	50	2.617 KE
74.125.236.167	10.189 KB	78	0 bps	4.161 KB	45	6.028 KE

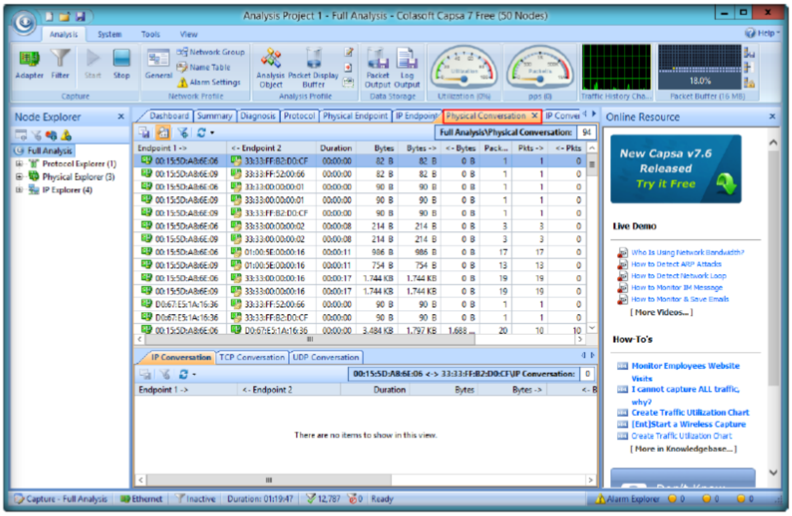
Local Subnet\IP Conversation: 56

Endpoint 1 ->	<- Endpoint 2	Duration	Bytes	Bytes ->	<- Bytes	Packets	Pkts ->	<- Pkts
10.0.0.2	74.125.236.173	00:02:22	4.821 KB	2.751 KB	2.070 KB	24	14	10
10.0.0.3	224.0.0.22	00:00:11	986 B	986 B	0 B	17	17	0
10.0.0.4	224.0.0.22	00:00:11	754 B	754 B	0 B	13	13	0
10.0.0.2	10.0.0.4	00:00:00	224 B	224 B	0 B	2	2	0
10.0.0.2	10.0.0.3	00:00:00	346 B	346 B	0 B	3	3	0
10.0.0.5	239.255.255.250	00:00:10	4.051 KB	4.051 KB	0 B	4	4	0

Capture - Full Analysis | Ethernet | Inactive | Duration: 01:16:14 | 12,387 | 0 | Ready

FIGURE 4.14: Colasoft Capsa Network Analyzer IP Endpoint view

17. The **Physical Conversation** tab presents the conversations between two MAC addresses.


Analysis Project 1 - Full Analysis - Colasoft Capsa 7 Free (50 Nodes)
Analysis
System
Tools
View
Adapter
Filter
Start
Stop
General
Network Group
Name Table
Alarm Settings
Analysis Object
Packet Display Buffer
Packet Output
Log Output
Network Profile
Analysis Profile
Data Storage
Node Explorer
Dashboard
Summary
Diagnosis
Protocol
Physical Endpoint
IP Endpoint
Physical Conversation
IP Conver
Online Resource
IP Conversation
TCP Conversation
UDP Conversation

Full Analysis\Physical Conversation: 94

Endpoint 1 ->	<- Endpoint 2	Duration	Bytes	Bytes ->	<- Bytes	Pack...	Pkts ->	<- Pkts
00:15:5D:A8:6E:06	33:33:FF:B2:D0:CF	00:00:00	82 B	82 B	0 B	1	1	0
00:15:5D:A8:6E:09	33:33:FF:52:00:66	00:00:00	82 B	82 B	0 B	1	1	0
00:15:5D:A8:6E:06	33:33:00:00:00:01	00:00:00	90 B	90 B	0 B	1	1	0
00:15:5D:A8:6E:09	33:33:00:00:00:01	00:00:00	90 B	90 B	0 B	1	1	0
00:15:5D:A8:6E:09	33:33:FF:B2:D0:CF	00:00:00	90 B	90 B	0 B	1	1	0
00:15:5D:A8:6E:06	33:33:00:00:00:02	00:00:08	214 B	214 B	0 B	3	3	0
00:15:5D:A8:6E:09	33:33:00:00:00:02	00:00:08	214 B	214 B	0 B	3	3	0
00:15:5D:A8:6E:06	01:00:5E:00:00:16	00:00:11	986 B	986 B	0 B	17	17	0
00:15:5D:A8:6E:09	01:00:5E:00:00:16	00:00:11	754 B	754 B	0 B	13	13	0
00:15:5D:A8:6E:06	33:33:00:00:00:16	00:00:17	1.744 KB	1.744 KB	0 B	19	19	0
00:15:5D:A8:6E:09	33:33:00:00:00:16	00:00:17	1.744 KB	1.744 KB	0 B	19	19	0
D0:67:E5:1A:16:36	33:33:FF:52:00:66	00:00:00	90 B	90 B	0 B	1	1	0
D0:67:E5:1A:16:36	33:33:FF:B2:D0:CF	00:00:00	90 B	90 B	0 B	1	1	0
00:15:5D:A8:6E:06	D0:67:E5:1A:16:36	00:00:00	3.484 KB	1.797 KB	1.688 ...	20	10	10

00:15:5D:A8:6E:06 <-> 33:33:FF:B2:D0:CF\IP Conversation: 0

Endpoint 1 ->	<- Endpoint 2	Duration	Bytes	Bytes ->	<- B

There are no items to show in this view.

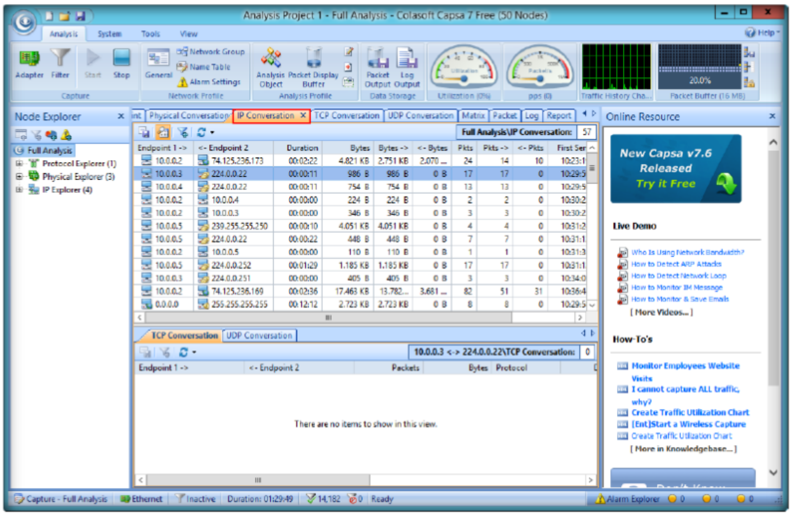
Capture - Full Analysis | Ethernet | Inactive | Duration: 01:19:47 | 12,787 | 0 | Ready

TTL tells the router whether the packet should be dropped if it stays in the network for too long. TTL is initially designed to define a time scope beyond which the packet is dropped. As TTL value is deducted by at least 1 by the router when the packet passes through, TTL often indicates the number of routers which the packet passed through before it was dropped.

FIGURE 4.15: Colasoft Capsa Network Analyzer Physical Conversations

18. The **IP Conversation** tab presents IP conversations between pairs of nodes.

19. The lower pane of the IP conversation section offers UDP and TCP conversation, which you can drill down to analyze.



Full Analysis\IP Conversation: 57

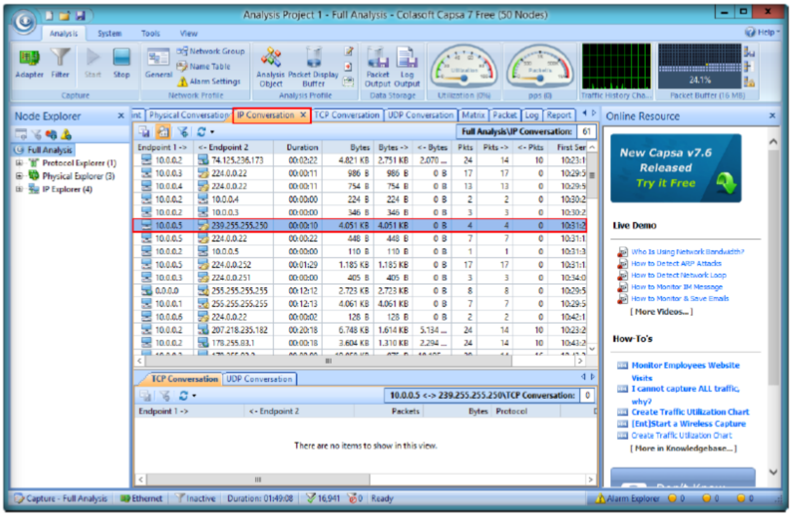
Endpoint 1 ->	<- Endpoint 2	Duration	Bytes	Bytes ->	<- Bytes	Pkts	Pkts ->	<- Pkts	First Ser
10.0.0.2	74.125.236.173	00:02:22	4.821 KB	2.751 KB	2.070 ...	24	14	10	10:23:1
10.0.0.3	224.0.0.22	00:00:11	986 B	986 B	0 B	17	17	0	10:29:5
10.0.0.4	224.0.0.22	00:00:11	754 B	754 B	0 B	13	13	0	10:29:5
10.0.0.2	10.0.0.4	00:00:00	224 B	224 B	0 B	2	2	0	10:30:2
10.0.0.2	10.0.0.3	00:00:00	346 B	346 B	0 B	3	3	0	10:30:2
10.0.0.5	239.255.255.250	00:00:10	4.051 KB	4.051 KB	0 B	4	4	0	10:31:2
10.0.0.5	224.0.0.22	00:00:22	448 B	448 B	0 B	7	7	0	10:31:1
10.0.0.2	10.0.0.5	00:00:00	110 B	110 B	0 B	1	1	0	10:31:3
10.0.0.5	224.0.0.252	00:01:29	1.185 KB	1.185 KB	0 B	17	17	0	10:31:1
10.0.0.3	224.0.0.251	00:00:00	405 B	405 B	0 B	3	3	0	10:34:0
10.0.0.2	74.125.236.169	00:02:36	17.463 KB	13.782...	3.681 ...	82	51	31	10:36:4
0.0.0.0	255.255.255.255	00:12:12	2.723 KB	2.723 KB	0 B	8	8	0	10:29:5

10.0.0.3 <-> 224.0.0.22\TCP Conversation: 0

There are no items to show in this view.

FIGURE 4.16: Colasoft Capsa Network Analyzer IP Conversations

20. Double-click a conversation in the **IP Conversation** list to view the full analysis of packets between two IPs. Here we are checking the conversation between 10.0.0.5 and 239.255.255.250.



Full Analysis\IP Conversation: 61

Endpoint 1 ->	<- Endpoint 2	Duration	Bytes	Bytes ->	<- Bytes	Pkts	Pkts ->	<- Pkts	First Ser
10.0.0.2	74.125.236.173	00:02:22	4.821 KB	2.751 KB	2.070 ...	24	14	10	10:23:1
10.0.0.3	224.0.0.22	00:00:11	986 B	986 B	0 B	17	17	0	10:29:5
10.0.0.4	224.0.0.22	00:00:11	754 B	754 B	0 B	13	13	0	10:29:5
10.0.0.2	10.0.0.4	00:00:00	224 B	224 B	0 B	2	2	0	10:30:2
10.0.0.2	10.0.0.3	00:00:00	346 B	346 B	0 B	3	3	0	10:30:2
10.0.0.5	239.255.255.250	00:00:10	4.051 KB	4.051 KB	0 B	4	4	0	10:31:2
10.0.0.5	224.0.0.22	00:00:22	448 B	448 B	0 B	7	7	0	10:31:1
10.0.0.2	10.0.0.5	00:00:00	110 B	110 B	0 B	1	1	0	10:31:3
10.0.0.5	224.0.0.252	00:01:29	1.185 KB	1.185 KB	0 B	17	17	0	10:31:1
10.0.0.3	224.0.0.251	00:00:00	405 B	405 B	0 B	3	3	0	10:34:0
0.0.0.0	255.255.255.255	00:12:12	2.723 KB	2.723 KB	0 B	8	8	0	10:29:5
10.0.0.1	255.255.255.255	00:12:13	4.061 KB	4.061 KB	0 B	7	7	0	10:29:5
10.0.0.6	224.0.0.22	00:00:02	128 B	128 B	0 B	2	2	0	10:42:1
10.0.0.2	207.218.235.182	00:20:18	6.748 KB	1.614 KB	5.134 ...	24	14	10	10:23:2
10.0.0.2	178.255.83.1	00:00:18	3.604 KB	1.310 KB	2.294 ...	24	14	10	10:43:2

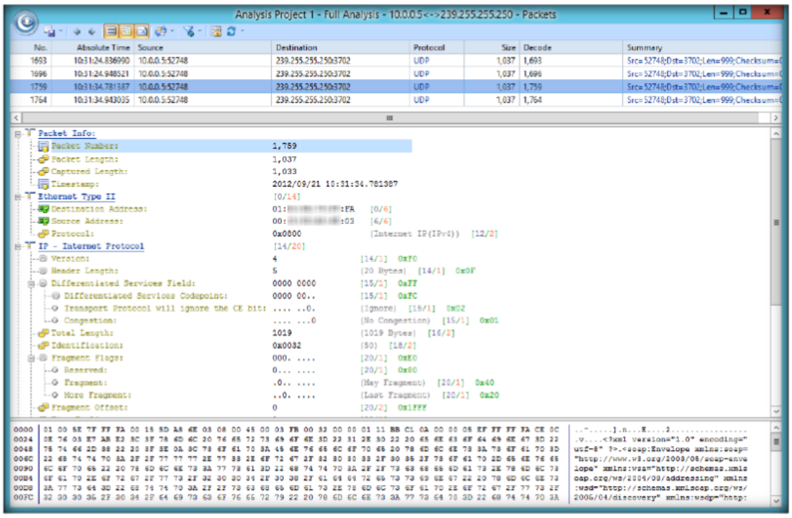
10.0.0.5 <-> 239.255.255.250\TCP Conversation: 0

There are no items to show in this view.

FIGURE 4.17: Colasoft Capsa Network Analyzer IP Conversations

21. A window opens displaying full packet analysis between 10.0.0.5 and 239.255.255.250.

A backdoor in a computer system (or cryptosystem or algorithm) is a method of bypassing normal authentication, securing remote access to a computer, obtaining access to plaintext, and so on. While attempting to remain undetected, the backdoor may take the form of an installed program or could be a modification to an existing program or hardware device.


Analysis Project 1 - Full Analysis - 10.0.0.5<->239.255.255.250 - Packets

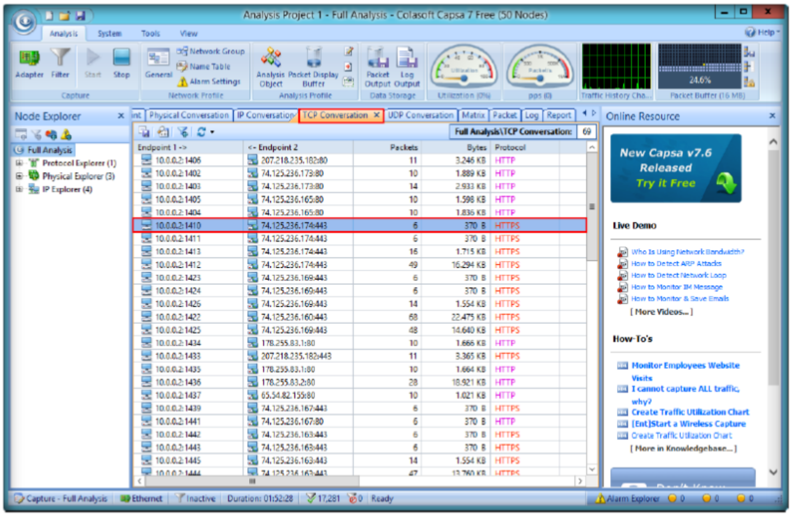
No.	Absolute Time	Source	Destination	Protocol	Size	Decode	Summary
1693	10:31:24.836990	10.0.0.5:52748	239.255.255.250:3702	UDP	1,037	1,693	Src=52748;Dst=3702;Len=999;Checksum=
1696	10:31:24.948521	10.0.0.5:52748	239.255.255.250:3702	UDP	1,037	1,696	Src=52748;Dst=3702;Len=999;Checksum=
1759	10:31:34.781387	10.0.0.5:52748	239.255.255.250:3702	UDP	1,037	1,759	Src=52748;Dst=3702;Len=999;Checksum=
1764	10:31:34.943035	10.0.0.5:52748	239.255.255.250:3702	UDP	1,037	1,764	Src=52748;Dst=3702;Len=999;Checksum=

```
Packet Info:
    Packet Number:                                  1,759
    Packet Length:                                  1,037
    Captured Length:                                1,033
    Timestamp:                                      2012/09/21 10:31:34.781387
Ethernet Type II                                    [0/14]
    Destination Address:                            01:[redacted]:FA   [0/6]
    Source Address:                                 00:[redacted]:03   [6/6]
    Protocol:                                       0x0800             (Internet IP(IPv4))  [12/2]
IP - Internet Protocol                              [14/20]
    Version:                                        4                  [14/1]  0xF0
    Header Length:                                  5                  (20 Bytes)  [14/1]  0x0F
    Differentiated Services Field:                  0000 0000          [15/1]  0xFF
        Differentiated Services Codepoint:          0000 00..          [15/1]  0xFC
        Transport Protocol will ignore the CE bit:  .... ..0.          (Ignore)  [15/1]  0x02
        Congestion:                                 .... ...0          (No Congestion)  [15/1]  0x01
    Total Length:                                   1019               (1019 Bytes)  [16/2]
    Identification:                                 0x0032             (50)  [18/2]
    Fragment Flags:                                 000. ....          [20/1]  0xE0
        Reserved:                                   0... ....          [20/1]  0x80
        Fragment:                                   .0.. ....          (May Fragment)  [20/1]  0x40
        More Fragment:                              ..0. ....          (Last Fragment)  [20/1]  0x20
    Fragment Offset:                                0                  [20/2]  0x1FFF
```

FIGURE 4.18: Full Packet Analysis of Nodes in IP Conversations

22. The **TCP Conversation** tab dynamically presents the real-time status of TCP conversations between pairs of nodes.

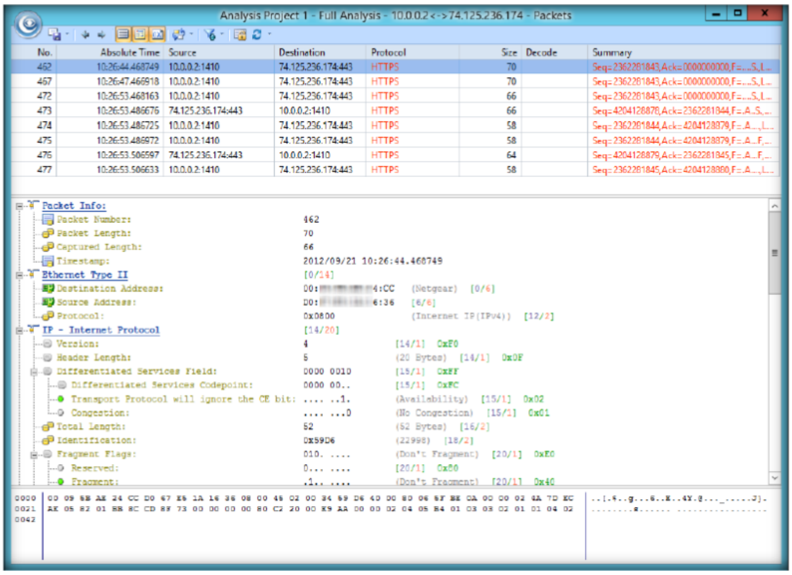
23. Double-click a node to display the full analysis of packets.


Analysis Project 1 - Full Analysis - Colasoft Capsa 7 Free (50 Nodes)
Analysis
System
Tools
View
Help
Adapter
Filter
Start
Stop
Capture
General
Network Group
Name Table
Alarm Settings
Network Profile
Analysis Object
Packet Display Buffer
Analysis Profile
Packet Output
Log Output
Data Storage
Utilization (0%)
pps (0)
Traffic History Cha...
24.6%
Packet Buffer (16 MB)
Node Explorer
Full Analysis
Protocol Explorer (1)
Physical Explorer (3)
IP Explorer (4)
Physical Conversation
IP Conversation
TCP Conversation
UDP Conversation
Matrix
Packet
Log
Report
Full Analysis\TCP Conversation: 69
Online Resource
New Capsa v7.6 Released Try it Free
Live Demo
Who Is Using Network Bandwidth?
How to Detect ARP Attacks
How to Detect Network Loop
How to Monitor IM Message
How to Monitor & Save Emails
[More Videos...]
How-To's
Monitor Employees Website Visits
I cannot capture ALL traffic, why?
Create Traffic Utilization Chart
[Ent]Start a Wireless Capture
Create Traffic Utilization Chart
[More in Knowledgebase...]
Capture - Full Analysis
Ethernet
Inactive
Duration: 01:52:28
17,281
0
Ready
Alarm Explorer

Endpoint 1 ->	<- Endpoint 2	Packets	Bytes	Protocol
10.0.0.2:1406	207.218.235.182:80	11	3.246 KB	HTTP
10.0.0.2:1402	74.125.236.173:80	10	1.889 KB	HTTP
10.0.0.2:1403	74.125.236.173:80	14	2.933 KB	HTTP
10.0.0.2:1405	74.125.236.165:80	10	1.598 KB	HTTP
10.0.0.2:1404	74.125.236.165:80	10	1.836 KB	HTTP
10.0.0.2:1410	74.125.236.174:443	6	370 B	HTTPS
10.0.0.2:1411	74.125.236.174:443	6	370 B	HTTPS
10.0.0.2:1413	74.125.236.174:443	16	1.715 KB	HTTPS
10.0.0.2:1412	74.125.236.174:443	49	16.294 KB	HTTPS
10.0.0.2:1423	74.125.236.169:443	6	370 B	HTTPS
10.0.0.2:1424	74.125.236.169:443	6	370 B	HTTPS
10.0.0.2:1426	74.125.236.169:443	14	1.554 KB	HTTPS
10.0.0.2:1422	74.125.236.160:443	68	22.475 KB	HTTPS
10.0.0.2:1425	74.125.236.169:443	48	14.640 KB	HTTPS
10.0.0.2:1434	178.255.83.1:80	10	1.666 KB	HTTP
10.0.0.2:1433	207.218.235.182:443	11	3.365 KB	HTTPS
10.0.0.2:1435	178.255.83.1:80	10	1.664 KB	HTTP
10.0.0.2:1436	178.255.83.2:80	28	18.921 KB	HTTP
10.0.0.2:1437	65.54.82.155:80	10	1.021 KB	HTTP
10.0.0.2:1439	74.125.236.167:443	6	370 B	HTTPS
10.0.0.2:1441	74.125.236.167:80	6	370 B	HTTP
10.0.0.2:1442	74.125.236.163:443	6	370 B	HTTPS
10.0.0.2:1443	74.125.236.163:443	6	370 B	HTTPS
10.0.0.2:1445	74.125.236.163:443	14	1.554 KB	HTTPS
10.0.0.2:1444	74.125.236.163:443	47	13.760 KB	HTTPS

FIGURE 4.19: Colasoft Capsa Network Analyzer TCP Conversations

24. A **Full Analysis** window is opened displaying detailed information of conversation between two nodes.


Analysis Project 1 - Full Analysis - 10.0.0.2<->74.125.236.174 - Packets

No.	Absolute Time	Source	Destination	Protocol	Size	Decode	Summary
462	10:26:44.468749	10.0.0.2:1410	74.125.236.174:443	HTTPS	70		Seq=2362281843,Ack=000000000,F=...S.,L...
467	10:26:47.466918	10.0.0.2:1410	74.125.236.174:443	HTTPS	70		Seq=2362281843,Ack=000000000,F=...S.,L...
472	10:26:53.468163	10.0.0.2:1410	74.125.236.174:443	HTTPS	66		Seq=2362281843,Ack=000000000,F=...S.,L...
473	10:26:53.486676	74.125.236.174:443	10.0.0.2:1410	HTTPS	66		Seq=4204128878,Ack=2362281844,F=.A..S.,...
474	10:26:53.486725	10.0.0.2:1410	74.125.236.174:443	HTTPS	58		Seq=2362281844,Ack=4204128879,F=.A...,L...
475	10:26:53.486972	10.0.0.2:1410	74.125.236.174:443	HTTPS	58		Seq=2362281844,Ack=4204128879,F=.A...F,...
476	10:26:53.506597	74.125.236.174:443	10.0.0.2:1410	HTTPS	64		Seq=4204128879,Ack=2362281845,F=.A...F,...
477	10:26:53.506633	10.0.0.2:1410	74.125.236.174:443	HTTPS	58		Seq=2362281845,Ack=4204128880,F=.A...,L...

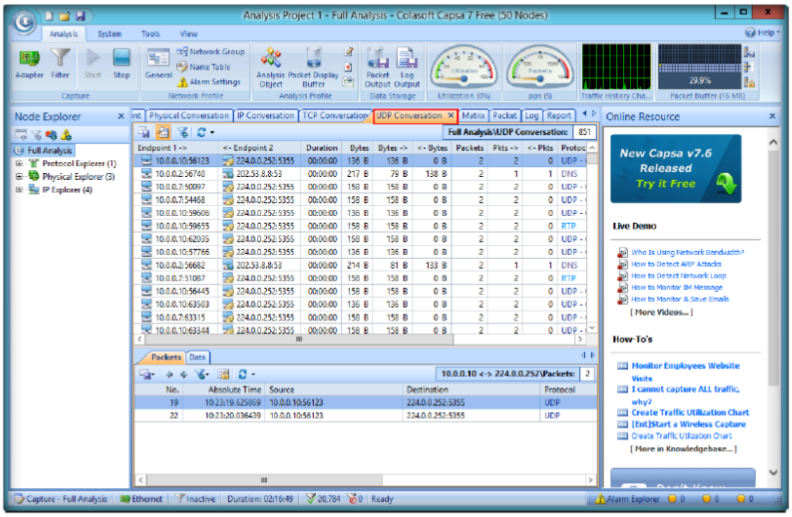
```
Packet Info:
    Packet Number:                              462
    Packet Length:                              70
    Captured Length:                            66
    Timestamp:                                  2012/09/21 10:26:44.468749
Ethernet Type II                                [0/14]
    Destination Address:                        D0:[redacted]4:CC      (Netgear)   [0/6]
    Source Address:                             D0:[redacted]6:36      [6/6]
    Protocol:                                   0x0800                 (Internet IP(IPv4))   [12/2]
IP - Internet Protocol                          [14/20]
    Version:                                    4                [14/1]   0xF0
    Header Length:                              5                (20 Bytes)   [14/1]   0x0F
    Differentiated Services Field:              0000 0010        [15/1]   0xFF
        Differentiated Services Codepoint:      0000 00..        [15/1]   0xFC
        Transport Protocol will ignore the CE bit:  .... ..1.    (Availability)   [15/1]   0x02
        Congestion:                             .... ...0        (No Congestion)   [15/1]   0x01
    Total Length:                               52               (52 Bytes)   [16/2]
    Identification:                             0x59D6           (22998)   [18/2]
    Fragment Flags:                             010. ....        (Don't Fragment)   [20/1]   0xE0
        Reserved:                               0... ....        [20/1]   0x80
        Fragment:                               .1.. ....        (Don't Fragment)   [20/1]   0x40
```

```
0000 | 00 09 5B AE 24 CC D0 67 E5 1A 16 36 08 00 45 02 00 34 59 D6 40 00 80 06 5F BE 0A 00 00 02 4A 7D EC | ..[.$..g...6..E..4Y.@..._.....J}.
0021 | AE 05 82 01 BB 8C CD 8F 73 00 00 00 00 80 C2 20 00 E9 AA 00 00 02 04 05 B4 01 03 03 02 01 01 04 02 | ........s...... ...............
0042 |
```

FIGURE 4.20: Full Packet Analysis of Nodes in TCP Conversations

25. The **UDP Conversation** tab dynamically presents the real-time status of UDP conversations between two nodes.

26. The lower pane of this tab gives you related packets and reconstructed data flow to help you drill down to analyze the conversations.


Analysis Project 1 - Full Analysis - Colasoft Capsa 7 Free (50 Nodes)
Analysis
System
Tools
View
Help
Adapter
Filter
Start
Stop
General
Network Group
Name Table
Alarm Settings
Analysis Object
Packet Display Buffer
Packet Output
Log Output
Capture
Network Profile
Analysis Profile
Data Storage
Utilization (0%)
pps (5)
Traffic History Cha...
29.9%
Packet Buffer (16 MB)
Node Explorer
Full Analysis
Protocol Explorer (1)
Physical Explorer (3)
IP Explorer (4)
Physical Conversation
IP Conversation
TCP Conversation
UDP Conversation
Matrix
Packet
Log
Report
Full Analysis\UDP Conversation: 851
Online Resource
New Capsa v7.6 Released
Try it Free
Live Demo
Who Is Using Network Bandwidth?
How to Detect ARP Attacks
How to Detect Network Loop
How to Monitor IM Message
How to Monitor & Save Emails
[More Videos...]
How-To's
Monitor Employees Website Visits
I cannot capture ALL traffic, why?
Create Traffic Utilization Chart
[Ent]Start a Wireless Capture
Create Traffic Utilization Chart
[More in Knowledgebase...]
Packets
Data
10.0.0.10 <-> 224.0.0.252\Packets: 2
Capture - Full Analysis
Ethernet
Inactive
Duration: 02:16:49
20,784
0
Ready
Alarm Explorer

Endpoint 1 ->	<- Endpoint 2	Duration	Bytes	Bytes ->	<- Bytes	Packets	Pkts ->	<- Pkts	Protoc
10.0.0.10:56123	224.0.0.252:5355	00:00:00	136 B	136 B	0 B	2	2	0	UDP -
10.0.0.2:56740	202.53.8.8:53	00:00:00	217 B	79 B	138 B	2	1	1	DNS
10.0.0.7:50097	224.0.0.252:5355	00:00:00	158 B	158 B	0 B	2	2	0	UDP -
10.0.0.7:54468	224.0.0.252:5355	00:00:00	158 B	158 B	0 B	2	2	0	UDP -
10.0.0.10:59606	224.0.0.252:5355	00:00:00	136 B	136 B	0 B	2	2	0	UDP -
10.0.0.10:59655	224.0.0.252:5355	00:00:00	158 B	158 B	0 B	2	2	0	RTP
10.0.0.10:62035	224.0.0.252:5355	00:00:00	158 B	158 B	0 B	2	2	0	UDP -
10.0.0.10:57766	224.0.0.252:5355	00:00:00	136 B	136 B	0 B	2	2	0	UDP -
10.0.0.2:56682	202.53.8.8:53	00:00:00	214 B	81 B	133 B	2	1	1	DNS
10.0.0.7:51087	224.0.0.252:5355	00:00:00	158 B	158 B	0 B	2	2	0	RTP
10.0.0.10:56445	224.0.0.252:5355	00:00:00	158 B	158 B	0 B	2	2	0	UDP -
10.0.0.10:63503	224.0.0.252:5355	00:00:00	136 B	136 B	0 B	2	2	0	UDP -
10.0.0.7:63315	224.0.0.252:5355	00:00:00	158 B	158 B	0 B	2	2	0	UDP -
10.0.0.10:63344	224.0.0.252:5355	00:00:00	158 B	158 B	0 B	2	2	0	UDP -

No.	Absolute Time	Source	Destination	Protocol
19	10:23:19.625869	10.0.0.10:56123	224.0.0.252:5355	UDP
22	10:23:20.036439	10.0.0.10:56123	224.0.0.252:5355	UDP

FIGURE 4.21: Colasoft Capsa Network Analyzer UDP Conversations

In networking, an email worm is a computer worm that can copy itself to the shared folder in a system and keeps sending infected emails to stochastic email addresses. In this way, it spreads fast via SMTP mail servers.

27. On the **Matrix** tab, you can view the nodes communicating in the network by connecting them in lines graphically.

28. The weight of the line indicates the volume of traffic between nodes arranged in an extensive ellipse.

29. You can easily navigate and shift between global statistics and details of specific network nodes by switching the corresponding nodes in the **Node Explorer** window.

Once we encounter the network malfunction or attack, the most important thing we should pay attention to is the current total network traffic, sent/received traffic, network connection, etc., to get a clear direction to find the problem. All of these statistics are included in the endpoint tabs in ColasoftCapsa.

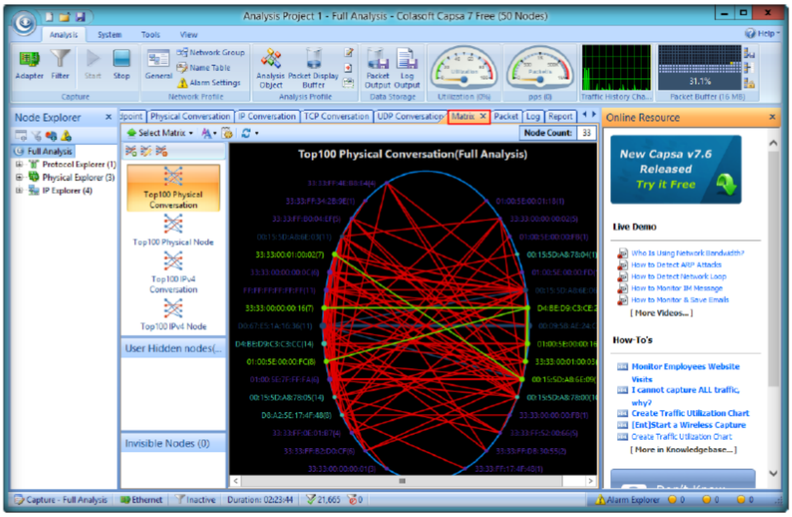
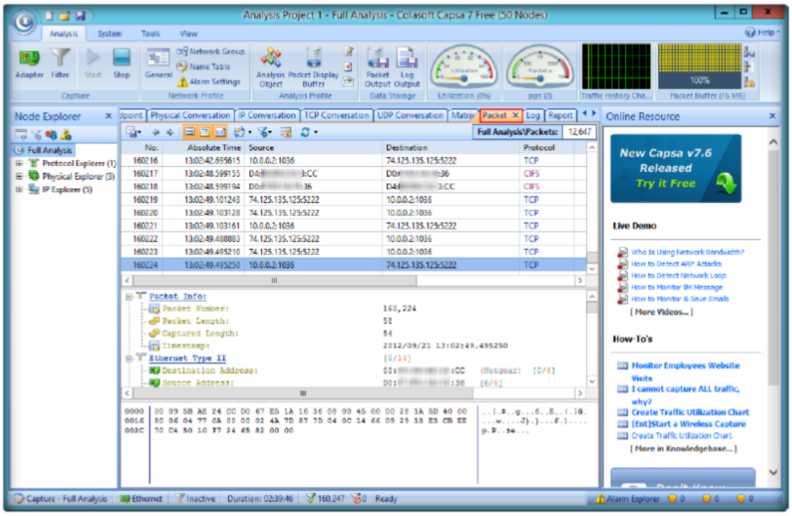

Analysis Project 1 - Full Analysis - Colasoft Capsa 7 Free (50 Nodes)
Analysis
System
Tools
View
Help
Adapter
Filter
Start
Stop
Capture
General
Network Group
Name Table
Alarm Settings
Network Profile
Analysis Object
Packet Display Buffer
Analysis Profile
Packet Output
Log Output
Data Storage
Utilization (0%)
pps (0)
Traffic History Cha...
31.1%
Packet Buffer (16 MB)
Node Explorer
Full Analysis
Protocol Explorer (1)
Physical Explorer (3)
IP Explorer (4)
Physical Conversation
IP Conversation
TCP Conversation
UDP Conversation
Matrix
Packet
Log
Report
Select Matrix
Node Count: 33
Top100 Physical Conversation
Top100 Physical Node
Top100 IPv4 Conversation
Top100 IPv4 Node
User Hidden nodes
Invisible Nodes (0)
Top100 Physical Conversation(Full Analysis)
Online Resource
New Capsa v7.6 Released Try it Free
Live Demo
Who Is Using Network Bandwidth?
How to Detect ARP Attacks
How to Detect Network Loop
How to Monitor IM Message
How to Monitor & Save Emails
[More Videos...]
How-To's
Monitor Employees Website Visits
I cannot capture ALL traffic, why?
Create Traffic Utilization Chart
[Ent]Start a Wireless Capture
Create Traffic Utilization Chart
[More in Knowledgebase...]
Capture - Full Analysis
Ethernet
Inactive
Duration: 02:23:44
21,665
0
Alarm Explorer

FIGURE 4.22: Colasoft Capsa Network Analyzer Matrix view

30. The **Packet** tab provides the original information for any packet. Double-click a packet to view the full analysis information of packet decode.

Protocols may be implemented by hardware, software, or a combination of the two. At the lowest level, a protocol defines the behavior of a hardware connection. A protocol is a formal description of message formats and the rules for exchanging those messages.


Analysis Project 1 - Full Analysis - Colasoft Capsa 7 Free (50 Nodes)
Analysis
System
Tools
View
Help
Adapter
Filter
Start
Stop
Capture
General
Network Group
Name Table
Alarm Settings
Network Profile
Analysis Object
Packet Display Buffer
Analysis Profile
Packet Output
Log Output
Data Storage
Utilization (0%)
pps (2)
Traffic History Cha...
100%
Packet Buffer (16 MB)
Node Explorer
Full Analysis
Protocol Explorer (1)
Physical Explorer (3)
IP Explorer (5)
Physical Conversation
IP Conversation
TCP Conversation
UDP Conversation
Matrix
Packet
Log
Report
Full Analysis\Packets: 12,647
Online Resource
New Capsa v7.6 Released Try it Free
Live Demo
Who Is Using Network Bandwidth?
How to Detect ARP Attacks
How to Detect Network Loop
How to Monitor IM Message
How to Monitor & Save Emails
[More Videos...]
How-To's
Monitor Employees Website Visits
I cannot capture ALL traffic, why?
Create Traffic Utilization Chart
[Ent]Start a Wireless Capture
Create Traffic Utilization Chart
[More in Knowledgebase...]
Capture - Full Analysis
Ethernet
Inactive
Duration: 02:39:46
160,247
0
Ready
Alarm Explorer

No.	Absolute Time	Source	Destination	Protocol
160216	13:02:42.695615	10.0.0.2:1036	74.125.135.125:5222	TCP
160217	13:02:48.599155	D4:[redacted]3:CC	D0:[redacted]:36	CIFS
160218	13:02:48.599194	D0:[redacted]:36	D4:[redacted]3:CC	CIFS
160219	13:02:49.101243	74.125.135.125:5222	10.0.0.2:1036	TCP
160220	13:02:49.103128	74.125.135.125:5222	10.0.0.2:1036	TCP
160221	13:02:49.103161	10.0.0.2:1036	74.125.135.125:5222	TCP
160222	13:02:49.488883	74.125.135.125:5222	10.0.0.2:1036	TCP
160223	13:02:49.495210	74.125.135.125:5222	10.0.0.2:1036	TCP
160224	13:02:49.495250	10.0.0.2:1036	74.125.135.125:5222	TCP

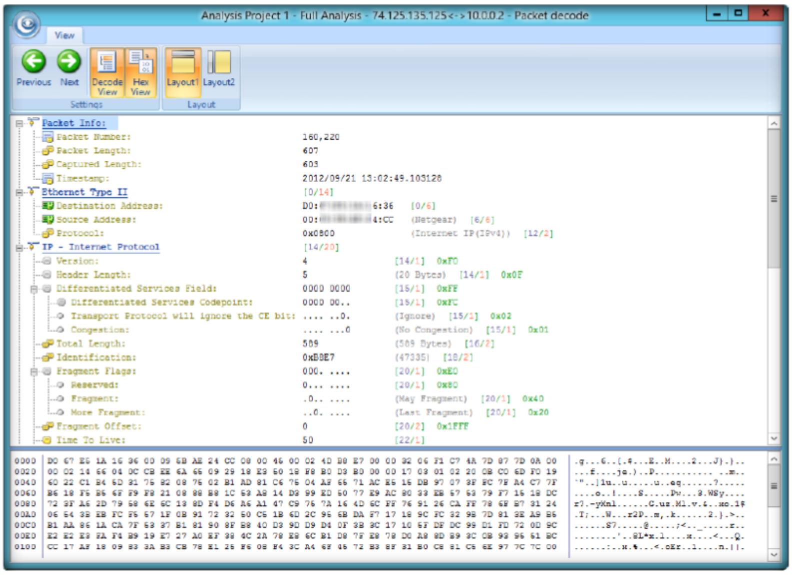
```
Packet Info:
    Packet Number:              160,224
    Packet Length:              58
    Captured Length:            54
    Timestamp:                  2012/09/21 13:02:49.495250
Ethernet Type II                [0/14]
    Destination Address:        00:[redacted]:CC   (Netgear)   [0/6]
    Source Address:             D0:[redacted]:36   [6/6]
```

```
0000  00 09 5B AE 24 CC D0 67 E5 1A 16 36 08 00 45 00 00 28 1A 5D 40 00
0016  80 06 04 77 0A 00 00 02 4A 7D 87 7D 04 0C 14 66 05 25 18 E5 CB EE
002C  70 C4 50 10 F7 24 65 82 00 00
```

FIGURE 4.23: Colasoft Capsa Network Analyzer Packet information

31. The Packet decode consists of two major parts: **Hex View** and **Decode View**.

Protocol decoding is the basic functionality as well. There is a Packet tab, which collect all captured packets or traffic. Select a packet and we can see its hex digits as well as the meaning of each field. The figure below shows the structure of an ARP packet. This makes it easy to understand how the packet is encapsulated according to its protocol rule.


Analysis Project 1 - Full Analysis - 74.125.135.125<->10.0.0.2 - Packet decode
View
Previous
Next
Decode View
Hex View
Settings
Layout1
Layout2
Layout

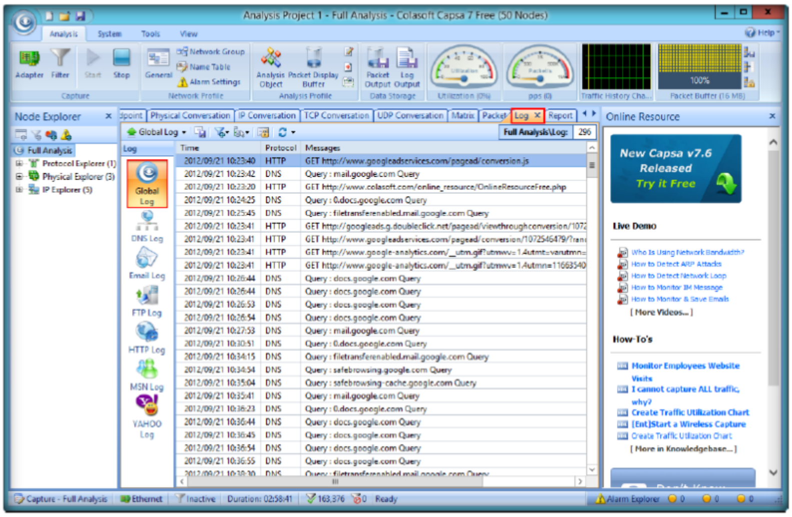
```
Packet Info:
  Packet Number:                                    160,220
  Packet Length:                                    607
  Captured Length:                                  603
  Timestamp:                                        2012/09/21 13:02:49.103128
Ethernet Type II                                    [0/14]
  Destination Address:                              D0:[redacted]6:36    [0/6]
  Source Address:                                   00:[redacted]4:CC    (Netgear)   [6/6]
  Protocol:                                         0x0800               (Internet IP(IPv4))   [12/2]
IP - Internet Protocol                              [14/20]
  Version:                                          4                [14/1]   0xF0
  Header Length:                                    5                (20 Bytes)   [14/1]   0x0F
  Differentiated Services Field:                    0000 0000        [15/1]   0xFF
    Differentiated Services Codepoint:              0000 00..        [15/1]   0xFC
    Transport Protocol will ignore the CE bit:      .... ..0.        (Ignore)   [15/1]   0x02
    Congestion:                                     .... ...0        (No Congestion)   [15/1]   0x01
  Total Length:                                     589              (589 Bytes)   [16/2]
  Identification:                                   0xB8E7           (47335)   [18/2]
  Fragment Flags:                                   000. ....        [20/1]   0xE0
    Reserved:                                       0... ....        [20/1]   0x80
    Fragment:                                       .0.. ....        (May Fragment)   [20/1]   0x40
    More Fragment:                                  ..0. ....        (Last Fragment)   [20/1]   0x20
  Fragment Offset:                                  0                [20/2]   0x1FFF
  Time To Live:                                     50               [22/1]
```

```
0000  D0 67 E5 1A 16 36 00 09 6B AE 24 CC 08 00 45 00 02 4D B8 E7 00 00 32 06 F1 C7 4A 7D 87 7D 0A 00
0020  00 02 14 66 04 DC CB EE 6A 65 09 29 18 E3 50 18 F8 B0 D3 B0 00 00 17 03 01 02 20 0B C0 6D F0 19
0040  60 22 C1 B4 6D 31 75 B2 08 75 02 B1 AD 81 C6 75 04 AF 66 71 AC E5 16 DB 97 07 3F EC 7E A4 C7 7F
0060  B6 18 F5 B6 6F F9 F8 21 08 88 B8 1C 53 A8 14 D3 99 ED 50 77 E9 AC 80 33 EB 57 53 79 F7 16 18 DC
0080  72 3F A6 2D 79 58 6E 6C 13 8D F4 D6 A6 A1 47 C9 76 7A 16 4D 6C FF 76 91 26 CA FF 78 6F B7 31 24
00A0  06 54 3B EB FC F6 57 1F 0B 91 72 32 50 C5 1B 6D 2C 95 6B DA F7 17 18 9C FC 32 9B 7D 81 3E A9 B6
00C0  B1 AA 86 1A CA 7F 53 37 B1 81 90 8F B8 40 D3 9D D9 D4 0F 3B 3C 17 10 6F DF DC 99 D1 FD 72 0D 9C
00E0  E2 E2 E3 FA F4 B9 19 E7 27 A0 EF 38 4C 2A 78 E8 6C B1 D8 7F E8 78 D0 A8 8D B9 3C 0B 93 96 61 BC
0100  CC 17 AF 18 09 B3 3A B3 CB 78 E1 25 F6 08 F4 3C A4 6F 45 72 B3 8F 31 B0 C8 81 C5 6E 97 7C 7C 00
```

FIGURE 4.24: Full Analysis of Packet Decode

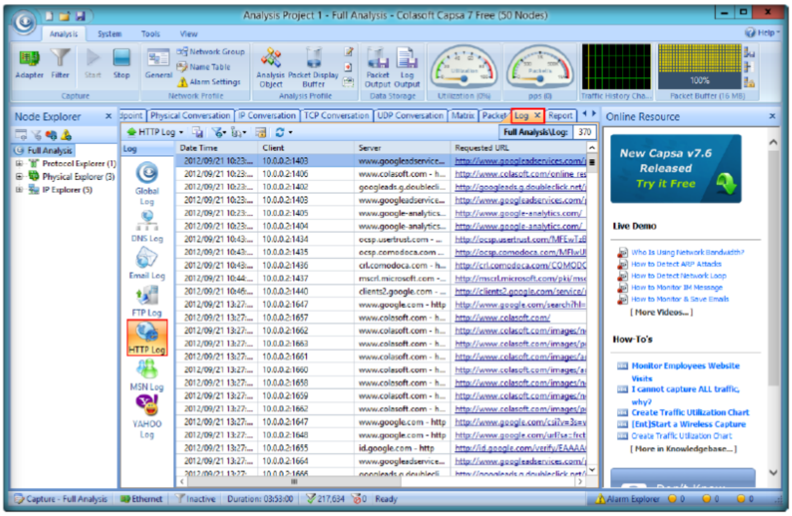
32. The **Log** tab provides a **Global Log**, **DNS Log**, **Email Log**, **FTP Log**, **HTTP Log**, **MSN Log** and **Yahoo Log**.

33. You can view the logs of **TCP conversations**, **Web access**, **DNS transactions**, **Email communications**, etc.


Analysis Project 1 - Full Analysis - Colasoft Capsa 7 Free (50 Nodes)
Analysis
System
Tools
View
Help
Adapter
Filter
Start
Stop
Capture
General
Network Group
Name Table
Alarm Settings
Network Profile
Analysis Object
Packet Display Buffer
Analysis Profile
Packet Output
Log Output
Data Storage
Utilization (0%)
pps (0)
Traffic History Chart
100%
Packet Buffer (16 MB)
Node Explorer
Full Analysis
Protocol Explorer (1)
Physical Explorer (3)
IP Explorer (5)
Endpoint
Physical Conversation
IP Conversation
TCP Conversation
UDP Conversation
Matrix
Packet
Log
Report
Global Log
Full Analysis\Log:
296
Log
Global Log
DNS Log
Email Log
FTP Log
HTTP Log
MSN Log
YAHOO Log
Online Resource
New Capsa v7.6 Released
Try it Free
Live Demo
Who Is Using Network Bandwidth?
How to Detect ARP Attacks
How to Detect Network Loop
How to Monitor IM Message
How to Monitor & Save Emails
[More Videos...]
How-To's
Monitor Employees Website Visits
I cannot capture ALL traffic, why?
Create Traffic Utilization Chart
[Ent]Start a Wireless Capture
Create Traffic Utilization Chart
[More in Knowledgebase...]
Capture - Full Analysis
Ethernet
Inactive
Duration: 02:58:41
163,376
0
Ready
Alarm Explorer
0
0
0

Time	Protocol	Messages
2012/09/21 10:23:40	HTTP	GET http://www.googleadservices.com/pagead/conversion.js
2012/09/21 10:23:42	DNS	Query : mail.google.com Query
2012/09/21 10:23:20	HTTP	GET http://www.colasoft.com/online_resource/OnlineResourceFree.php
2012/09/21 10:24:25	DNS	Query : 0.docs.google.com Query
2012/09/21 10:25:45	DNS	Query : filetransferenabled.mail.google.com Query
2012/09/21 10:23:41	HTTP	GET http://googleads.g.doubleclick.net/pagead/viewthroughconversion/1072
2012/09/21 10:23:41	HTTP	GET http://www.googleadservices.com/pagead/conversion/1072546479/?ran
2012/09/21 10:23:41	HTTP	GET http://www.google-analytics.com/__utm.gif?utmwv=1.4utmt=varutmn=
2012/09/21 10:23:41	HTTP	GET http://www.google-analytics.com/__utm.gif?utmwv=1.4utmn=11663540
2012/09/21 10:26:44	DNS	Query : docs.google.com Query
2012/09/21 10:26:44	DNS	Query : docs.google.com Query
2012/09/21 10:26:53	DNS	Query : docs.google.com Query
2012/09/21 10:26:54	DNS	Query : docs.google.com Query
2012/09/21 10:27:53	DNS	Query : mail.google.com Query
2012/09/21 10:30:51	DNS	Query : 0.docs.google.com Query
2012/09/21 10:34:15	DNS	Query : filetransferenabled.mail.google.com Query
2012/09/21 10:34:54	DNS	Query : safebrowsing.google.com Query
2012/09/21 10:35:04	DNS	Query : safebrowsing-cache.google.com Query
2012/09/21 10:35:41	DNS	Query : mail.google.com Query
2012/09/21 10:36:23	DNS	Query : 0.docs.google.com Query
2012/09/21 10:36:44	DNS	Query : docs.google.com Query
2012/09/21 10:36:45	DNS	Query : docs.google.com Query
2012/09/21 10:36:54	DNS	Query : docs.google.com Query
2012/09/21 10:36:55	DNS	Query : docs.google.com Query
2012/09/21 10:38:30	DNS	Query : filetransferenabled.mail.google.com Query

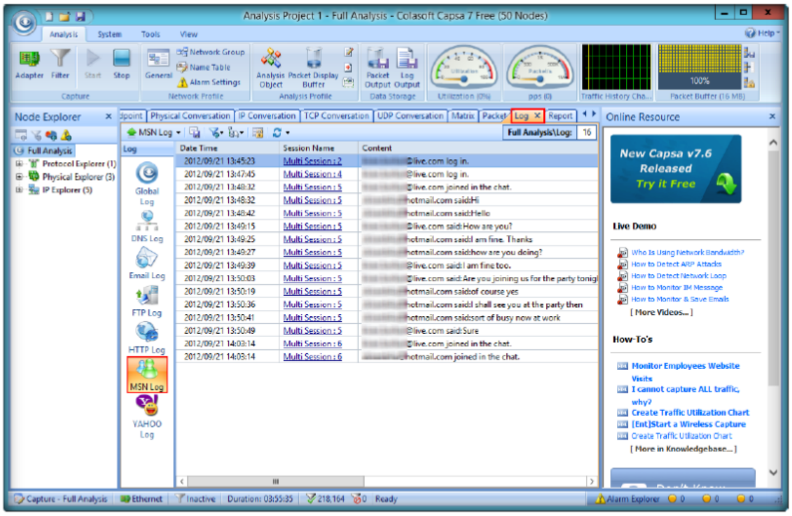
FIGURE 4.25: Colasoft Capsa Network Analyzer Global Log view


Analysis Project 1 - Full Analysis - Colasoft Capsa 7 Free (50 Nodes)
Analysis
System
Tools
View
Adapter
Filter
Start
Stop
General
Network Group
Name Table
Alarm Settings
Analysis Object
Packet Display Buffer
Packet Output
Log Output
Node Explorer
Full Analysis
Protocol Explorer (1)
Physical Explorer (3)
IP Explorer (5)
Physical Conversation
IP Conversation
TCP Conversation
UDP Conversation
Matrix
Packet
Log
Report
HTTP Log
Full Analysis\Log: 370
Global Log
DNS Log
Email Log
FTP Log
HTTP Log
MSN Log
YAHOO Log
Online Resource
New Capsa v7.6 Released Try it Free
Live Demo
How-To's
Capture - Full Analysis
Ethernet
Inactive
Duration: 03:53:00
217,634
0
Ready
Alarm Explorer

Date Time	Client	Server	Requested URL
2012/09/21 10:23:...	10.0.0.2:1403	www.googleadservice...	http://www.googleadservices.com/
2012/09/21 10:23:...	10.0.0.2:1406	www.colasoft.com - h...	http://www.colasoft.com/online_res
2012/09/21 10:23:...	10.0.0.2:1402	googleads.g.doublecli...	http://googleads.g.doubleclick.net/
2012/09/21 10:23:...	10.0.0.2:1403	www.googleadservice...	http://www.googleadservices.com/
2012/09/21 10:23:...	10.0.0.2:1405	www.google-analytics...	http://www.google-analytics.com/
2012/09/21 10:23:...	10.0.0.2:1404	www.google-analytics...	http://www.google-analytics.com/
2012/09/21 10:43:...	10.0.0.2:1434	ocsp.usertrust.com - ...	http://ocsp.usertrust.com/MFEwTzB
2012/09/21 10:43:...	10.0.0.2:1435	ocsp.comodoca.com ...	http://ocsp.comodoca.com/MFIwUI
2012/09/21 10:43:...	10.0.0.2:1436	crl.comodoca.com - h...	http://crl.comodoca.com/COMODC
2012/09/21 10:44:...	10.0.0.2:1437	mscrl.microsoft.com -...	http://mscrl.microsoft.com/pki/msc
2012/09/21 10:46:...	10.0.0.2:1440	clients2.google.com - ...	http://clients2.google.com/service/
2012/09/21 13:27:...	10.0.0.2:1647	www.google.com - http	http://www.google.com/search?hl=
2012/09/21 13:27:...	10.0.0.2:1657	www.colasoft.com - h...	http://www.colasoft.com/
2012/09/21 13:27:...	10.0.0.2:1662	www.colasoft.com - h...	http://www.colasoft.com/images/n
2012/09/21 13:27:...	10.0.0.2:1663	www.colasoft.com - h...	http://www.colasoft.com/images/p
2012/09/21 13:27:...	10.0.0.2:1661	www.colasoft.com - h...	http://www.colasoft.com/images/a
2012/09/21 13:27:...	10.0.0.2:1660	www.colasoft.com - h...	http://www.colasoft.com/images/a
2012/09/21 13:27:...	10.0.0.2:1658	www.colasoft.com - h...	http://www.colasoft.com/images/n
2012/09/21 13:27:...	10.0.0.2:1659	www.colasoft.com - h...	http://www.colasoft.com/images/n
2012/09/21 13:27:...	10.0.0.2:1662	www.colasoft.com - h...	http://www.colasoft.com/images/p
2012/09/21 13:27:...	10.0.0.2:1647	www.google.com - http	http://www.google.com/csi?v=3s=v
2012/09/21 13:27:...	10.0.0.2:1648	www.google.com - http	http://www.google.com/url?sa=t&rct
2012/09/21 13:27:...	10.0.0.2:1655	id.google.com - http	http://id.google.com/verify/EAAAA
2012/09/21 13:27:...	10.0.0.2:1664	www.googleadservice...	http://www.googleadservices.com/

FIGURE 4.26: Colasoft Capsa Network Analyzer HTTP Log view

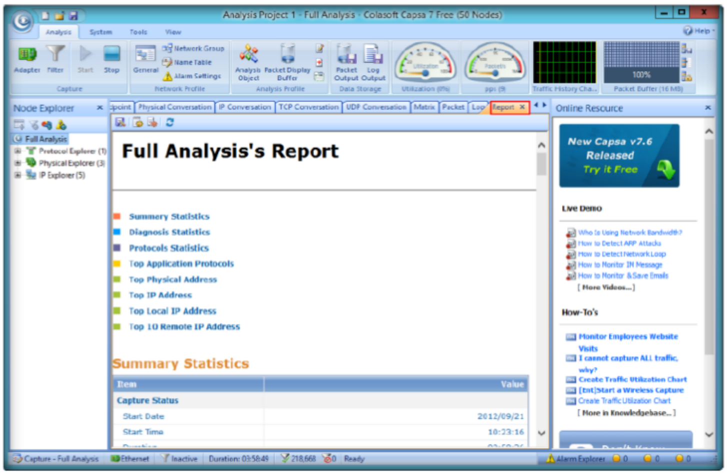
34. If you have MSN or Yahoo Messenger running on your system, you can view the MSN and Yahoo logs.


Analysis Project 1 - Full Analysis - Colasoft Capsa 7 Free (50 Nodes)
Analysis
System
Tools
View
Node Explorer
Full Analysis
Protocol Explorer (1)
Physical Explorer (3)
IP Explorer (5)
Log
Report
MSN Log
Full Analysis\Log: 16
Global Log
DNS Log
Email Log
FTP Log
HTTP Log
MSN Log
YAHOO Log
Online Resource
New Capsa v7.6 Released Try it Free
Live Demo
How-To's
Capture - Full Analysis
Ethernet
Inactive
Duration: 03:55:35
218,164
0
Ready
Alarm Explorer

Date Time	Session Name	Content
2012/09/21 13:45:23	Multi Session : 2	[redacted]@live.com log in.
2012/09/21 13:47:45	Multi Session : 4	[redacted]@live.com log in.
2012/09/21 13:48:32	Multi Session : 5	[redacted]@live.com joined in the chat.
2012/09/21 13:48:32	Multi Session : 5	[redacted]hotmail.com said:Hi
2012/09/21 13:48:42	Multi Session : 5	[redacted]hotmail.com said:Hello
2012/09/21 13:49:15	Multi Session : 5	[redacted]@live.com said:How are you?
2012/09/21 13:49:25	Multi Session : 5	[redacted]hotmail.com said:I am fine. Thanks
2012/09/21 13:49:27	Multi Session : 5	[redacted]hotmail.com said:how are you doing?
2012/09/21 13:49:39	Multi Session : 5	[redacted]@live.com said:I am fine too.
2012/09/21 13:50:03	Multi Session : 5	[redacted]@live.com said:Are you joining us for the party tonig
2012/09/21 13:50:19	Multi Session : 5	[redacted]hotmail.com said:of course yes
2012/09/21 13:50:36	Multi Session : 5	[redacted]hotmail.com said:I shall see you at the party then
2012/09/21 13:50:41	Multi Session : 5	[redacted]hotmail.com said:sort of busy now at work
2012/09/21 13:50:49	Multi Session : 5	[redacted]@live.com said:Sure
2012/09/21 14:03:14	Multi Session : 6	[redacted]@live.com joined in the chat.
2012/09/21 14:03:14	Multi Session : 6	[redacted]hotmail.com joined in the chat.

FIGURE 4.27: Colasoft Capsa Network Analyzer MSN Log view

35. The **Report** tab provides 27 statistics reports from the global network to a specific network node.



Full Analysis's Report

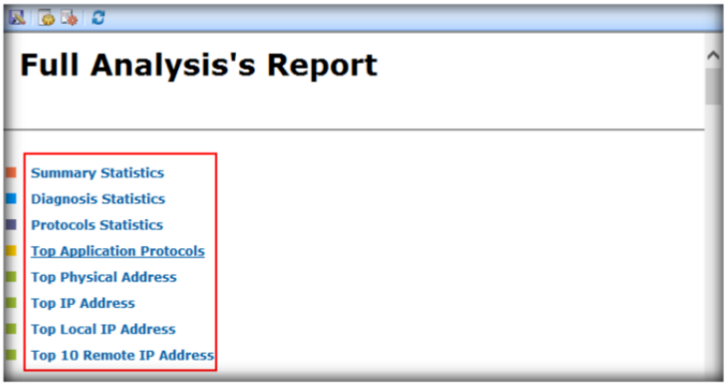
- Summary Statistics
- Diagnosis Statistics
- Protocols Statistics
- Top Application Protocols
- Top Physical Address
- Top IP Address
- Top Local IP Address
- Top 10 Remote IP Address

Summary Statistics

Item	Value
Capture Status	
Start Date	2012/09/21
Start Time	10:23:16

FIGURE 4.28: Colasoft Capsa Network Analyzer Full Analysis's Report

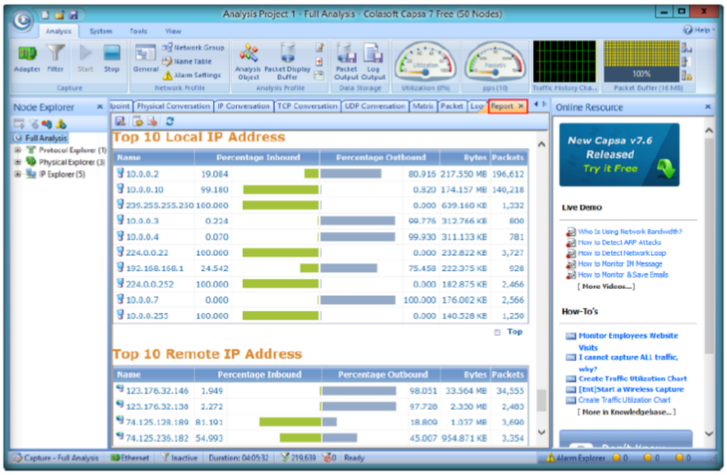
36. You can click the respective hyperlinks for information or you can scroll down to view the complete detailed report.



Full Analysis's Report

- Summary Statistics
- Diagnosis Statistics
- Protocols Statistics
- Top Application Protocols
- Top Physical Address
- Top IP Address
- Top Local IP Address
- Top 10 Remote IP Address

Almost all Trojans and worms need an access to the network, because they have to return data to the hacker. Only the useful data are sent for the Trojan to accomplish its mission. So it is a good solution to start from the aspect of traffic analysis and protocol analysis technology.



Top 10 Local IP Address

Name	Percentage Inbound	Percentage Outbound	Bytes	Packets
10.0.0.2	19.084	80.916	217.550 MB	196,612
10.0.0.10	99.180	0.820	174.157 MB	140,218
239.255.255.250	100.000	0.000	639.160 KB	1,332
10.0.0.3	0.224	99.776	312.766 KB	800
10.0.0.4	0.070	99.930	311.133 KB	781
224.0.0.22	100.000	0.000	232.822 KB	3,727
192.168.168.1	24.542	75.458	222.375 KB	928
224.0.0.252	100.000	0.000	182.875 KB	2,466
10.0.0.7	0.000	100.000	176.002 KB	2,566
10.0.0.255	100.000	0.000	140.528 KB	1,250

Top

Top 10 Remote IP Address

Name	Percentage Inbound	Percentage Outbound	Bytes	Packets
123.176.32.146	1.949	98.051	33.564 MB	34,555
123.176.32.138	2.272	97.728	2.330 MB	2,483
74.125.128.189	81.191	18.809	1.037 MB	3,690
74.125.236.182	54.993	45.007	954.871 KB	3,354

FIGURE 4.29: Colasoft Capsa Network Analyzer Full Analysis's Report

37. Click **Stop** on toolbar after completing your task.

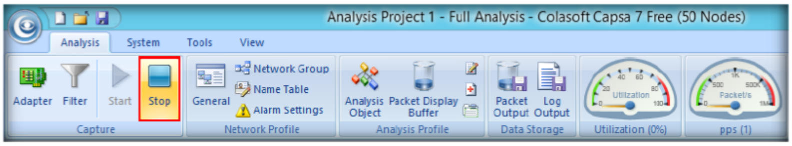

Analysis Project 1 - Full Analysis - Colasoft Capsa 7 Free (50 Nodes)
Analysis
System
Tools
View
Adapter
Filter
Start
Stop
Capture
General
Network Group
Name Table
Alarm Settings
Network Profile
Analysis Object
Packet Display Buffer
Analysis Profile
Packet Output
Log Output
Data Storage
Utilization
Utilization (0%)
Packet/s
pps (1)

FIGURE 4.30: Colasoft Capsa Network Analyzer Stopping process

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure through public and free information.

Tool/Utility	Information Collected/Objectives Achieved
Capsa Network Analyzer	**Diagnosis:** ▪ Name ▪ Physical Address ▪ IP Address
	Packet Info: ▪ Packet Number ▪ Packet Length ▪ Captured Length
	Ethernet Type: ▪ Destination Address ▪ Source Address ▪ Protocol ▪ Physical Endpoint ▪ IP Endpoint
	Conversations: ▪ Physical Conversation ▪ IP Conversation ▪ TCP Conversation ▪ UDP Conversation
	Logs: ▪ Global Log ▪ DNS Log ▪ Email Log ▪ FTP Log ▪ HTTP Log ▪ MSN Log ▪ Yahoo Log

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Analyze how Capsa affects your network traffic, while analyzing the network.
2. What types of instant messages does Capsa monitor?
3. Determine if the packet buffer will affect performance. If yes, then what steps can you take to avoid or reduce its effect on software?

Internet Connection Required	
☑ **Yes**	☐ No
Platform Supported	
☑ **Classroom**	☐ iLabs

Lab
5

Sniffing Passwords Using Wireshark

Wireshark is a network packet analyzer. A network packet analyzer will try to capture network packets and display packet data in detail.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

As in the previous lab, you are able to capture TCP and UDP conversations; an attacker, too, can collect this information and perform attacks on a network. Attackers listen to the conversation occurring between two hosts and issue packets using the same source IP address. Attackers will first know the IP address and correct sequence number by monitoring the traffic. Once the attacker has control over the connection, he or she then sends counterfeit packets. These sorts of attacks can cause various types of damage, including the injection into an existing TCP connection of data and the premature closure of an existing TCP connection by the injection of counterfeit packets with the FIN bit set.

As an administrator you can configure a firewall or router to prevent the damage caused by such attacks. To be an expert **ethical hacker** and **penetration tester**, you must have sound knowledge of sniffing network packets, performing ARP poisoning, spoofing the network, and DNS poisoning. Another use of a packet analyzer is to sniff passwords, which you will learn about in this lab using the Wireshark packet analyzer.

Lab Objectives

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 08 Sniffing

The objective of this lab is to demonstrate the **sniffing** technique to capture from **multiple** interfaces and data collection from any network topology.

Lab Environment

In the lab you will need:

- **Wireshark** located at **D:\CEH-Tools\CEHv8 Module 08 Sniffing\Sniffing Tools\Wireshark**

- You can also download the latest version of **WireShark** from the link http://www.wireshark.org/download.html
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- A computer running **Windows Server 2012** as Host (Attacker) machine
- A virtual machine (Windows 8 or Windows 2008 Server) as a Victim machine
- A web browser with Internet connection
- Double-click **Wireshark-win64-1.8.2.exe** and follow the wizard-driven installation steps to install WireShark
- **Administrative** privileges to run tools

You can download Wireshark from http://www.wireshark.org.

Lab Duration

Time: 20 Minutes

Overview of Password Sniffing

Password sniffing uses various techniques to sniff network and get someone's password. Networks use **broadcast** technology to send data. Data **transmits** through the broadcast network, which can be read by anyone on the other computer present on the network. Usually, all the computers except the recipient of the message will notice that the **message** is not meant for them, and ignore it.

Many computers are **programmed** to look at every message on the network. If someone misuses the facility, they can view **message**, which is not intended of others.

Lab Tasks

TASK 1

Capturing Packet

1. Before starting this lab, login to the virtual machine(s).
2. On the host machine, launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

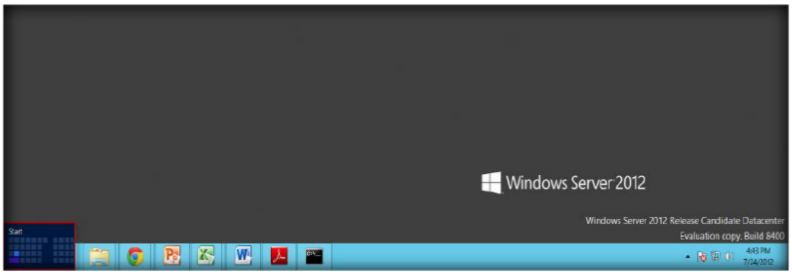

Start
Windows Server 2012
Windows Server 2012 Release Candidate Datacenter
Evaluation copy. Build 8400
4:43 PM
7/24/2012

FIGURE 5.1: Windows Server 2012 – Desktop view

3. Click **Wireshark** to launch the application.

Wireshark is an open source software project, and is released under the GNU General Public License (GPL)

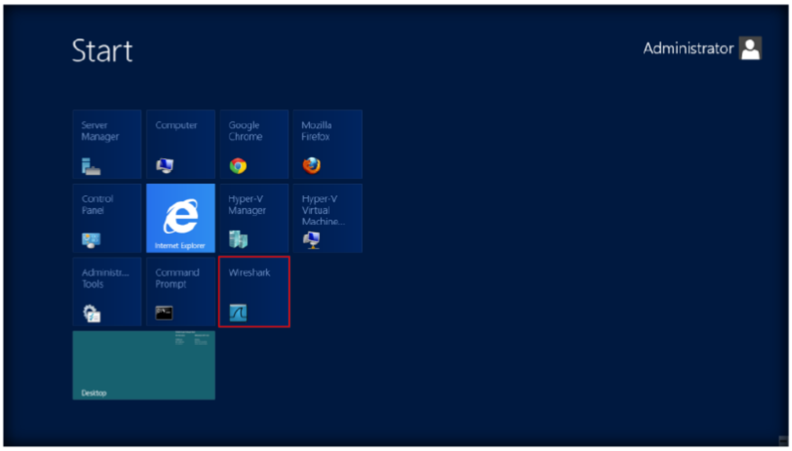

Start
Administrator
Server Manager
Computer
Google Chrome
Mozilla Firefox
Control Panel
Internet Explorer
Hyper-V Manager
Hyper-V Virtual Machine...
Administr... Tools
Command Prompt
Wireshark
Desktop

FIGURE 5.2: Windows Server 2012 – Desktop view

A network packet analyzer is a kind of measuring device used to examine what is going on inside a network cable, just like a voltmeter is used by an electrician to examine what's going on inside an electric cable (but at a higher level, of course).

4. The **Wireshark** main window appears.

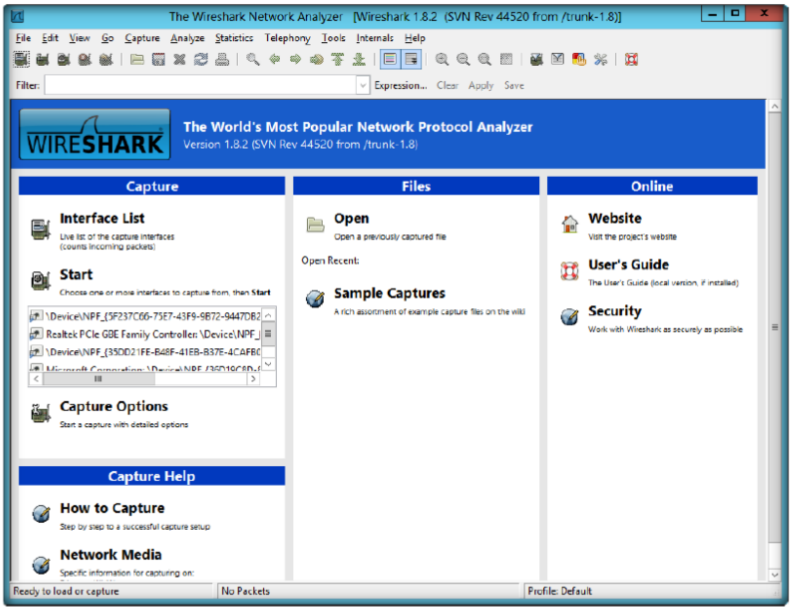

The Wireshark Network Analyzer [Wireshark 1.8.2 (SVN Rev 44520 from /trunk-1.8)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
WIRESHARK
The World's Most Popular Network Protocol Analyzer
Version 1.8.2 (SVN Rev 44520 from /trunk-1.8)
Capture
Interface List
Live list of the capture interfaces (counts incoming packets)
Start
Choose one or more interfaces to capture from, then Start
\Device\NPF_{5F237C66-75E7-43F9-9B72-9447DB2
Realtek PCIe GBE Family Controller: \Device\NPF_
\Device\NPF_{35DD21FE-B48F-41EB-B37E-4CAFBC
Microsoft Corporation: \Device\NPF_{35DD19C8D-
Capture Options
Start a capture with detailed options
Capture Help
How to Capture
Step by step to a successful capture setup
Network Media
Specific information for capturing on:
Files
Open
Open a previously captured file
Open Recent:
Sample Captures
A rich assortment of example capture files on the wiki
Online
Website
Visit the project's website
User's Guide
The User's Guide (local version, if installed)
Security
Work with Wireshark as securely as possible
Ready to load or capture
No Packets
Profile: Default

FIGURE 5.3: Wireshark Main Window

FIGURE 5.3: Wireshark Main Window

5. From the **Wireshark** menu bar, select **Capture → Interfaces (Ctrl+I)**.

Wireshark is used for:

Network administrators use it to troubleshoot network problems

- Network security engineers use it to examine security problems
- Developers use it to debug protocol implementations
- People use it to learn network protocol internals

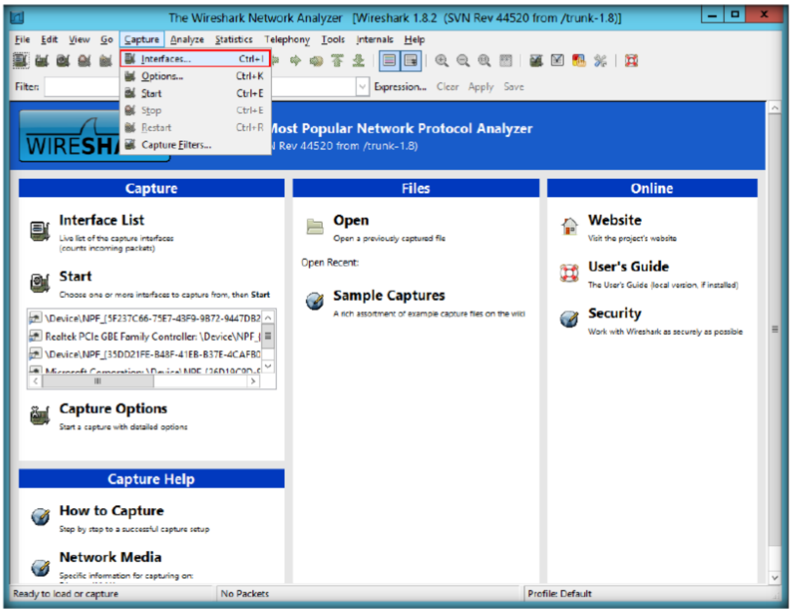
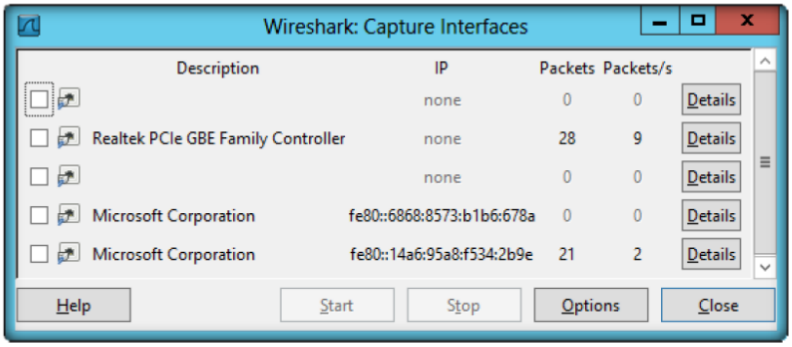

The Wireshark Network Analyzer [Wireshark 1.8.2 (SVN Rev 44520 from /trunk-1.8)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Interfaces... Ctrl+I
Options... Ctrl+K
Start Ctrl+E
Stop Ctrl+E
Restart Ctrl+R
Capture Filters...
Filter:
Expression... Clear Apply Save
WIRESHA
Most Popular Network Protocol Analyzer
Rev 44520 from /trunk-1.8)
Capture
Interface List
Live list of the capture interfaces (counts incoming packets)
Start
Choose one or more interfaces to capture from, then Start
\Device\NPF_{5F237C66-75E7-43F9-9872-9447DB2
Realtek PCIe GBE Family Controller: \Device\NPF_{
\Device\NPF_{35DD21FE-B48F-41EB-B37E-4CAFB0
Capture Options
Start a capture with detailed options
Capture Help
How to Capture
Step by step to a successful capture setup
Network Media
Specific information for capturing on:
Files
Open
Open a previously captured file
Open Recent:
Sample Captures
A rich assortment of example capture files on the wiki
Online
Website
Visit the project's website
User's Guide
The User's Guide (local version, if installed)
Security
Work with Wireshark as securely as possible
Ready to load or capture
No Packets
Profile: Default

FIGURE 5.4: Wireshark Main Window with Interface Option

Wireshark Features:

- Available for UNIX and Windows
- Capture live packet data from a network interface
- Display packets with very detailed protocol information
- Open and Save packet data captured
- Import and Export packet data from and to a lot of other capture programs

6. The **Wireshark Capture Interface** window appears.


Wireshark: Capture Interfaces
Help
Start
Stop
Options
Close

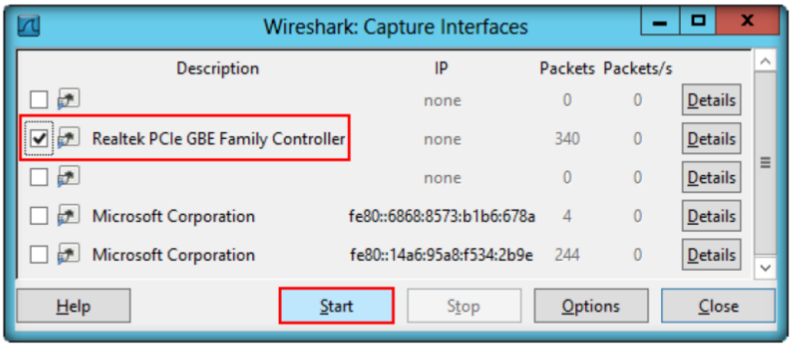
	Description	IP	Packets	Packets/s	
☐		none	0	0	Details
☐	Realtek PCIe GBE Family Controller	none	28	9	Details
☐		none	0	0	Details
☐	Microsoft Corporation	fe80::6868:8573:b1b6:678a	0	0	Details
☐	Microsoft Corporation	fe80::14a6:95a8:f534:2b9e	21	2	Details

FIGURE 5.5: Wireshark Capture Interfaces Window

7. In the **Wireshark Capture Interfaces** dialog box, find and select the **Ethernet Driver Interface** that is connected to the system.
8. In the previous screenshot, it is the **Realtek PCIe GBE Family Controller**. The interface should show some packets passing through it, as it is connected to the network.
9. Click **Start** in that interface's line.

Wireshark can capture traffic from many different network media types - and despite its name - including wireless LAN as well.

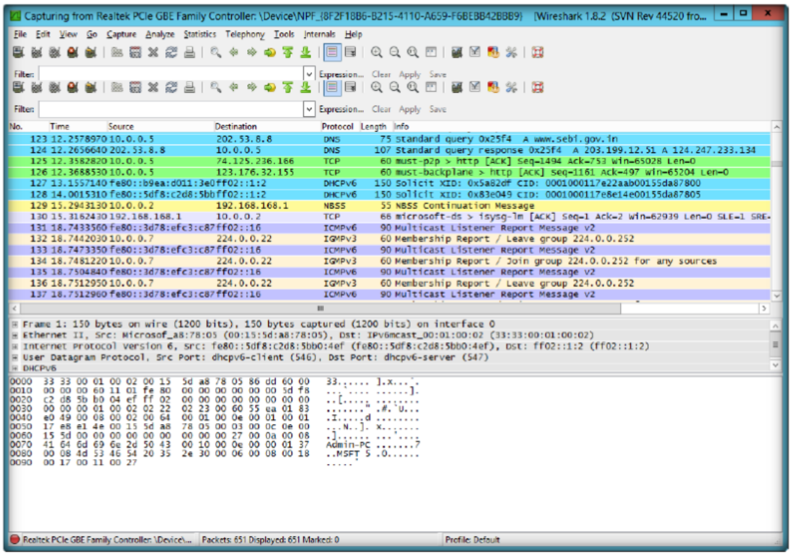
A supported network card for capturing: Ethernet: Any card supported by Windows should work. See the wiki pages on Ethernet capture and offloading for issues that may affect your environment.


Wireshark: Capture Interfaces
Help
Start
Stop
Options
Close

	Description	IP	Packets	Packets/s	
☐		none	0	0	Details
☑	Realtek PCIe GBE Family Controller	none	340	0	Details
☐		none	0	0	Details
☐	Microsoft Corporation	fe80::6868:8573:b1b6:678a	4	0	Details
☐	Microsoft Corporation	fe80::14a6:95a8:f534:2b9e	244	0	Details

FIGURE 5.6: Wireshark Capture Interfaces Window – Starting Capture

10. Traffic informs of packets generated through the computer while browsing the Internet.


Capturing from Realtek PCIe GBE Family Controller: \Device\NPF_{8F2F18B6-B215-4110-A659-F6BEBB42BBB9} [Wireshark 1.8.2 (SVN Rev 44520 fro...
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
Realtek PCIe GBE Family Controller: \Device\...
Packets: 651 Displayed: 651 Marked: 0
Profile: Default

```
No.  Time       Source                 Destination      Protocol Length Info
 123 12.2578970 10.0.0.5               202.53.8.8       DNS        75 Standard query 0x25f4  A www.sebi.gov.in
 124 12.2656640 202.53.8.8             10.0.0.5         DNS       107 Standard query response 0x25f4  A 203.199.12.51 A 124.247.233.134
 125 12.3582820 10.0.0.5               74.125.236.166   TCP        60 must-p2p > http [ACK] Seq=1494 Ack=753 Win=65028 Len=0
 126 12.3688530 10.0.0.5               123.176.32.155   TCP        60 must-backplane > http [ACK] Seq=1161 Ack=497 Win=65204 Len=0
 127 13.1557140 fe80::b9ea:d011:3e0ff02::1:2            DHCPv6    150 Solicit XID: 0x5a82df CID: 0001000117e22aab00155da87800
 128 14.0015310 fe80::5df8:c2d8:5bbff02::1:2            DHCPv6    150 Solicit XID: 0x83e049 CID: 0001000117e8e14e00155da87805
 129 15.2943130 10.0.0.2               192.168.168.1    NBSS       55 NBSS Continuation Message
 130 15.3162430 192.168.168.1          10.0.0.2         TCP        66 microsoft-ds > isysg-lm [ACK] Seq=1 Ack=2 Win=62939 Len=0 SLE=1 SRE=
 131 18.7433560 fe80::3d78:efc3:c87ff02::16             ICMPv6     90 Multicast Listener Report Message v2
 132 18.7442030 10.0.0.7               224.0.0.22       IGMPv3     60 Membership Report / Leave group 224.0.0.252
 133 18.7473350 fe80::3d78:efc3:c87ff02::16             ICMPv6     90 Multicast Listener Report Message v2
 134 18.7481220 10.0.0.7               224.0.0.22       IGMPv3     60 Membership Report / Join group 224.0.0.252 for any sources
 135 18.7504840 fe80::3d78:efc3:c87ff02::16             ICMPv6     90 Multicast Listener Report Message v2
 136 18.7512950 10.0.0.7               224.0.0.22       IGMPv3     60 Membership Report / Leave group 224.0.0.252
 137 18.7512960 fe80::3d78:efc3:c87ff02::16             ICMPv6     90 Multicast Listener Report Message v2
```

```
⊞ Frame 1: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits) on interface 0
⊞ Ethernet II, Src: Microsof_a8:78:05 (00:15:5d:a8:78:05), Dst: IPv6mcast_00:01:00:02 (33:33:00:01:00:02)
⊞ Internet Protocol Version 6, Src: fe80::5df8:c2d8:5bb0:4ef (fe80::5df8:c2d8:5bb0:4ef), Dst: ff02::1:2 (ff02::1:2)
⊞ User Datagram Protocol, Src Port: dhcpv6-client (546), Dst Port: dhcpv6-server (547)
⊞ DHCPv6
```

```
0000  33 33 00 01 00 02 00 15  5d a8 78 05 86 dd 60 00   33...... ].x...`.
0010  00 00 00 60 11 01 fe 80  00 00 00 00 00 00 5d f8   ...`.... ......].
0020  c2 d8 5b b0 04 ef ff 02  00 00 00 00 00 00 00 00   ..[..... ........
0030  00 00 00 01 00 02 02 22  02 23 00 60 55 ea 01 83   ......." .#.`U...
0040  e0 49 00 08 00 02 00 64  00 01 00 0e 00 01 00 01   .I.....d ........
0050  17 e8 e1 4e 00 15 5d a8  78 05 00 03 00 0c 0e 00   ...N..]. x.......
0060  15 5d 00 00 00 00 00 00  00 00 00 27 00 0a 00 08   .]...... ...'....
0070  41 64 6d 69 6e 2d 50 43  00 10 00 0e 00 00 01 37   Admin-PC .......7
0080  00 08 4d 53 46 54 20 35  2e 30 00 06 00 08 00 18   ..MSFT 5 .0......
0090  00 17 00 11 00 27                                  .....'
```

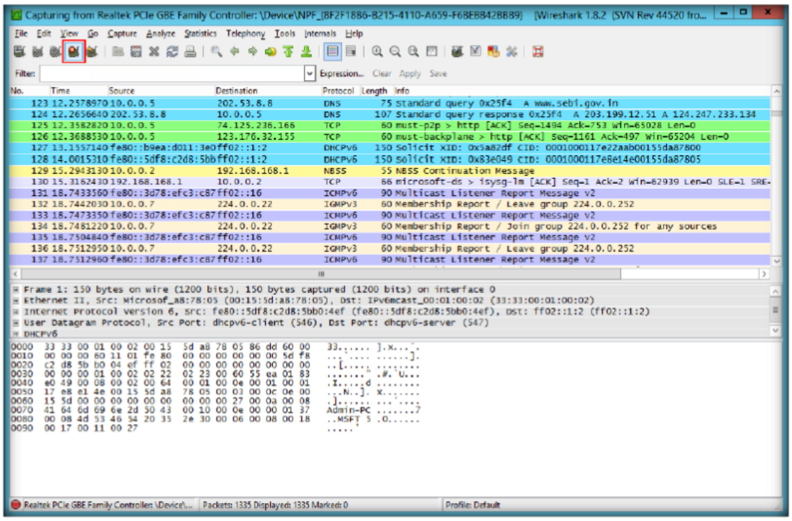
FIGURE 5.7: Wireshark Window with Packets Captured

11. Now, switch to the virtual machine and login to your email ID for which you would like to sniff the password.

TASK 2

Stop Live Capturing

12. Stop the running live capture by clicking the icon on the toolbar.


Capturing from Realtek PCIe GBE Family Controller: \Device\NPF_{8F2F1886-B215-4110-A659-F6BEBB42BBB9}   [Wireshark 1.8.2 (SVN Rev 44520 fro...
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

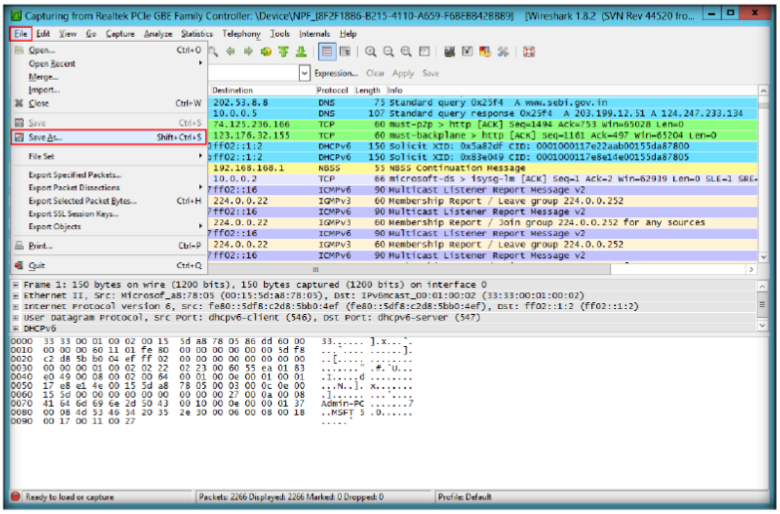
```
No.   Time       Source                   Destination       Protocol Length Info
  123 12.2578970 10.0.0.5                 202.53.8.8        DNS        75 Standard query 0x25f4  A www.sebi.gov.in
  124 12.2656640 202.53.8.8               10.0.0.5          DNS       107 Standard query response 0x25f4  A 203.199.12.51 A 124.247.233.134
  125 12.3582820 10.0.0.5                 74.125.236.166    TCP        60 must-p2p > http [ACK] Seq=1494 Ack=753 Win=65028 Len=0
  126 12.3688530 10.0.0.5                 123.176.32.155    TCP        60 must-backplane > http [ACK] Seq=1161 Ack=497 Win=65204 Len=0
  127 13.1557140 fe80::b9ea:d011:3e0ff02::1:2               DHCPv6    150 Solicit XID: 0x5a82df CID: 0001000117e22aab00155da87800
  128 14.0015310 fe80::5df8:c2d8:5bbff02::1:2               DHCPv6    150 Solicit XID: 0x83e049 CID: 0001000117e8e14e00155da87805
  129 15.2943130 10.0.0.2                 192.168.168.1     NBSS       55 NBSS Continuation Message
  130 15.3162430 192.168.168.1            10.0.0.2          TCP        66 microsoft-ds > isysg-lm [ACK] Seq=1 Ack=2 Win=62939 Len=0 SLE=1 SRE=
  131 18.7433560 fe80::3d78:efc3:c87ff02::16                ICMPv6     90 Multicast Listener Report Message v2
  132 18.7442030 10.0.0.7                 224.0.0.22        IGMPv3     60 Membership Report / Leave group 224.0.0.252
  133 18.7473350 fe80::3d78:efc3:c87ff02::16                ICMPv6     90 Multicast Listener Report Message v2
  134 18.7481220 10.0.0.7                 224.0.0.22        IGMPv3     60 Membership Report / Join group 224.0.0.252 for any sources
  135 18.7504840 fe80::3d78:efc3:c87ff02::16                ICMPv6     90 Multicast Listener Report Message v2
  136 18.7512950 10.0.0.7                 224.0.0.22        IGMPv3     60 Membership Report / Leave group 224.0.0.252
  137 18.7512960 fe80::3d78:efc3:c87ff02::16                ICMPv6     90 Multicast Listener Report Message v2

⊞ Frame 1: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits) on interface 0
⊞ Ethernet II, Src: Microsof_a8:78:05 (00:15:5d:a8:78:05), Dst: IPv6mcast_00:01:00:02 (33:33:00:01:00:02)
⊞ Internet Protocol Version 6, Src: fe80::5df8:c2d8:5bb0:4ef (fe80::5df8:c2d8:5bb0:4ef), Dst: ff02::1:2 (ff02::1:2)
⊞ User Datagram Protocol, Src Port: dhcpv6-client (546), Dst Port: dhcpv6-server (547)
⊞ DHCPv6

0000  33 33 00 01 00 02 00 15  5d a8 78 05 86 dd 60 00   33...... ].x...`.
0010  00 00 00 60 11 01 fe 80  00 00 00 00 00 00 5d f8   ...`.... ......].
0020  c2 d8 5b b0 04 ef ff 02  00 00 00 00 00 00 00 00   ..[..... ........
0030  00 00 00 01 00 02 02 22  02 23 00 60 55 ea 01 83   ......." .#.`U...
0040  e0 49 00 08 00 02 00 64  00 01 00 0e 00 01 00 01   .I.....d ........
0050  17 e8 e1 4e 00 15 5d a8  78 05 00 03 00 0c 0e 00   ...N..]. x.......
0060  15 5d 00 00 00 00 00 00  00 00 00 27 00 0a 00 08   .]...... ...'....
0070  41 64 6d 69 6e 2d 50 43  00 10 00 0e 00 00 01 37   Admin-PC .......7
0080  00 08 4d 53 46 54 20 35  2e 30 00 06 00 08 00 18   ..MSFT 5 .0......
0090  00 17 00 11 00 27                                  .....'

Realtek PCIe GBE Family Controller: \Device\...   Packets: 1335 Displayed: 1335 Marked: 0   Profile: Default
```

FIGURE 5.8: Wireshark Window – Stopping Live Capture

13. You may save the captured packets from **File → Save As**, provide a name for the file, and save it in the desired location

TASK 3

Saving Captured Files

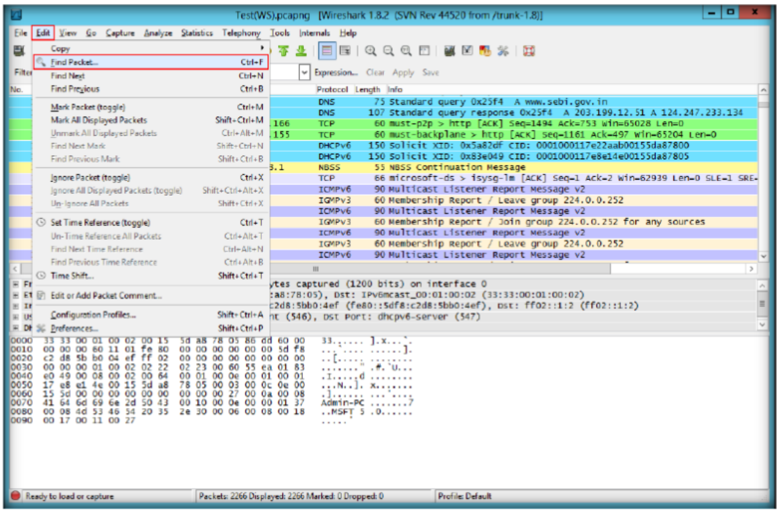

Capturing from Realtek PCIe GBE Family Controller: \Device\NPF_{8F2F1886-B215-4110-A659-F6BEBB42BBB9}   [Wireshark 1.8.2 (SVN Rev 44520 fro...
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Open... Ctrl+O
Open Recent
Merge...
Import...
Close Ctrl+W
Save Ctrl+S
Save As... Shift+Ctrl+S
File Set
Export Specified Packets...
Export Packet Dissections
Export Selected Packet Bytes... Ctrl+H
Export SSL Session Keys...
Export Objects
Print... Ctrl+P
Quit Ctrl+Q
Expression... Clear Apply Save

```
 Destination       Protocol Length Info
 202.53.8.8        DNS        75 Standard query 0x25f4  A www.sebi.gov.in
 10.0.0.5          DNS       107 Standard query response 0x25f4  A 203.199.12.51 A 124.247.233.134
 74.125.236.166    TCP        60 must-p2p > http [ACK] Seq=1494 Ack=753 Win=65028 Len=0
 123.176.32.155    TCP        60 must-backplane > http [ACK] Seq=1161 Ack=497 Win=65204 Len=0
0ff02::1:2         DHCPv6    150 Solicit XID: 0x5a82df CID: 0001000117e22aab00155da87800
bff02::1:2         DHCPv6    150 Solicit XID: 0x83e049 CID: 0001000117e8e14e00155da87805
 192.168.168.1     NBSS       55 NBSS Continuation Message
 10.0.0.2          TCP        66 microsoft-ds > isysg-lm [ACK] Seq=1 Ack=2 Win=62939 Len=0 SLE=1 SRE=
7ff02::16          ICMPv6     90 Multicast Listener Report Message v2
 224.0.0.22        IGMPv3     60 Membership Report / Leave group 224.0.0.252
7ff02::16          ICMPv6     90 Multicast Listener Report Message v2
 224.0.0.22        IGMPv3     60 Membership Report / Join group 224.0.0.252 for any sources
7ff02::16          ICMPv6     90 Multicast Listener Report Message v2
 224.0.0.22        IGMPv3     60 Membership Report / Leave group 224.0.0.252
7ff02::16          ICMPv6     90 Multicast Listener Report Message v2

⊞ Frame 1: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits) on interface 0
⊞ Ethernet II, Src: Microsof_a8:78:05 (00:15:5d:a8:78:05), Dst: IPv6mcast_00:01:00:02 (33:33:00:01:00:02)
⊞ Internet Protocol Version 6, Src: fe80::5df8:c2d8:5bb0:4ef (fe80::5df8:c2d8:5bb0:4ef), Dst: ff02::1:2 (ff02::1:2)
⊞ User Datagram Protocol, Src Port: dhcpv6-client (546), Dst Port: dhcpv6-server (547)
⊞ DHCPv6

0000  33 33 00 01 00 02 00 15  5d a8 78 05 86 dd 60 00   33...... ].x...`.
0010  00 00 00 60 11 01 fe 80  00 00 00 00 00 00 5d f8   ...`.... ......].
0020  c2 d8 5b b0 04 ef ff 02  00 00 00 00 00 00 00 00   ..[..... ........
0030  00 00 00 01 00 02 02 22  02 23 00 60 55 ea 01 83   ......." .#.`U...
0040  e0 49 00 08 00 02 00 64  00 01 00 0e 00 01 00 01   .I.....d ........
0050  17 e8 e1 4e 00 15 5d a8  78 05 00 03 00 0c 0e 00   ...N..]. x.......
0060  15 5d 00 00 00 00 00 00  00 00 00 27 00 0a 00 08   .]...... ...'....
0070  41 64 6d 69 6e 2d 50 43  00 10 00 0e 00 00 01 37   Admin-PC .......7
0080  00 08 4d 53 46 54 20 35  2e 30 00 06 00 08 00 18   ..MSFT 5 .0......
0090  00 17 00 11 00 27                                  .....'

Ready to load or capture   Packets: 2266 Displayed: 2266 Marked: 0 Dropped: 0   Profile: Default
```

FIGURE 5.9: WireShark – Saving the Captured Packets

14. Now, go to **Edit** and click **Find Packet...**

Wireshark can save packets captured in a large number of formats of other capture programs.

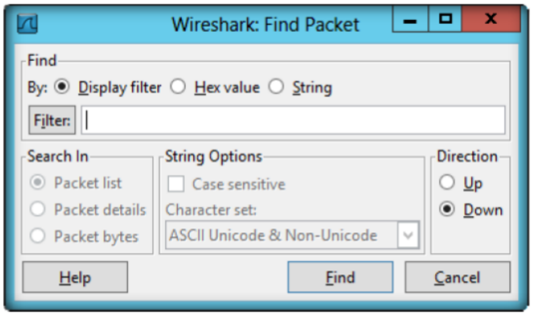

Test(WS).pcapng [Wireshark 1.8.2 (SVN Rev 44520 from /trunk-1.8)]
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Tools
Internals
Help
Copy
Find Packet... Ctrl+F
Find Next Ctrl+N
Find Previous Ctrl+B
Mark Packet (toggle) Ctrl+M
Mark All Displayed Packets Shift+Ctrl+M
Unmark All Displayed Packets Ctrl+Alt+M
Find Next Mark Shift+Ctrl+N
Find Previous Mark Shift+Ctrl+B
Ignore Packet (toggle) Ctrl+X
Ignore All Displayed Packets (toggle) Shift+Ctrl+Alt+X
Un-Ignore All Packets Shift+Ctrl+X
Set Time Reference (toggle) Ctrl+T
Un-Time Reference All Packets Ctrl+Alt+T
Find Next Time Reference Ctrl+Alt+N
Find Previous Time Reference Ctrl+Alt+B
Time Shift... Shift+Ctrl+T
Edit or Add Packet Comment...
Configuration Profiles... Shift+Ctrl+A
Preferences... Shift+Ctrl+P
Filter
Expression...
Clear
Apply
Save
No.
Protocol
Length
Info

```
                DNS      75 Standard query 0x25f4  A www.sebi.gov.in
                DNS     107 Standard query response 0x25f4  A 203.199.12.51 A 124.247.233.134
.166            TCP      60 must-p2p > http [ACK] Seq=1494 Ack=753 Win=65028 Len=0
.155            TCP      60 must-backplane > http [ACK] Seq=1161 Ack=497 Win=65204 Len=0
                DHCPv6  150 Solicit XID: 0x5a82df CID: 0001000117e22aab00155da87800
                DHCPv6  150 Solicit XID: 0x83e049 CID: 0001000117e8e14e00155da87805
3.1             NBSS     55 NBSS Continuation Message
                TCP      66 microsoft-ds > isysg-lm [ACK] Seq=1 Ack=2 Win=62939 Len=0 SLE=1 SRE-
                ICMPv6   90 Multicast Listener Report Message v2
                IGMPv3   60 Membership Report / Leave group 224.0.0.252
                ICMPv6   90 Multicast Listener Report Message v2
                IGMPv3   60 Membership Report / Join group 224.0.0.252 for any sources
                ICMPv6   90 Multicast Listener Report Message v2
                IGMPv3   60 Membership Report / Leave group 224.0.0.252
                ICMPv6   90 Multicast Listener Report Message v2

Fr ytes captured (1200 bits) on interface 0
Et :a8:78:05), Dst: IPv6mcast_00:01:00:02 (33:33:00:01:00:02)
Ir c2d8:5bb0:4ef (fe80::5df8:c2d8:5bb0:4ef), Dst: ff02::1:2 (ff02::1:2)
Us nt (546), Dst Port: dhcpv6-server (547)
Dh

0000  33 33 00 01 00 02 00 15  5d a8 78 05 86 dd 60 00   33...... ].x...`.
0010  00 00 00 60 11 01 fe 80  00 00 00 00 00 00 5d f8   ...`.... ......].
0020  c2 d8 5b b0 04 ef ff 02  00 00 00 00 00 00 00 00   ..[..... ........
0030  00 00 00 01 00 02 02 22  02 23 00 60 55 ea 01 83   ......." .#.`U...
0040  e0 49 00 08 00 02 00 64  00 01 00 0e 00 01 00 01   .I.....d ........
0050  17 e8 e1 4e 00 15 5d a8  78 05 00 03 00 0c 0e 00   ...N..]. x.......
0060  15 5d 00 00 00 00 00 00  00 00 00 27 00 0a 00 08   .]...... ...'....
0070  41 64 6d 69 6e 2d 50 43  00 10 00 0e 00 00 01 37   Admin-PC .......7
0080  00 08 4d 53 46 54 20 35  2e 30 00 06 00 08 00 18   ..MSFT 5 .0......
0090  00 17 00 11 00 27                                  .....'

Ready to load or capture | Packets: 2266 Displayed: 2266 Marked: 0 Dropped: 0 | Profile: Default
```

FIGURE 5.10: Wireshark – Finding Packet Option

Wireshark is not an intrusion detection system. It will not warn you when someone does strange things on your network that he/she isn't allowed to do. However, if strange things happen, Wireshark might help you figure out what is really going on.

15. The **Wireshark: Find Packet** window appears.

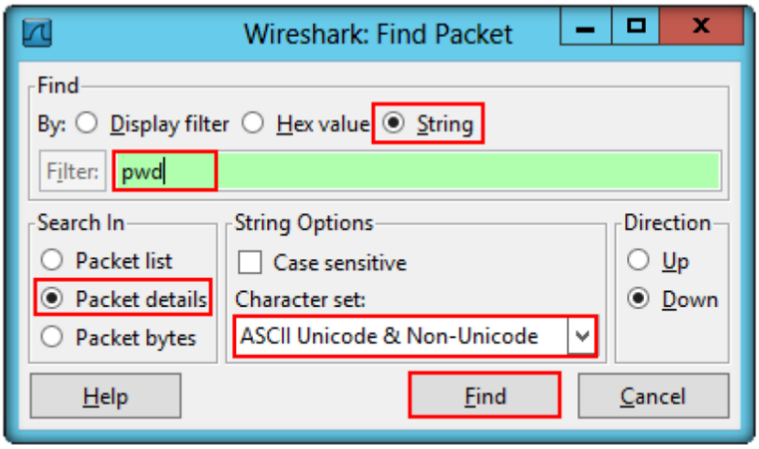

Wireshark: Find Packet
Find
By:
Display filter
Hex value
String
Filter:
Search In
Packet list
Packet details
Packet bytes
String Options
Case sensitive
Character set:
ASCII Unicode & Non-Unicode
Direction
Up
Down
Help
Find
Cancel

By: ● Display filter ○ Hex value ○ String

Direction: ○ Up ● Down

FIGURE 5.11: Wireshark – Find Packet Window

16. In **Find By**, select **String**, type **pwd** in the **Filter** field, select the radio button for **Packet details** under **Search In** and select **ASCII Unicode & Non-Unicode** from the **Character set** drop-down list. Click **Find**.


Wireshark: Find Packet
Find
Display filter
Hex value
Search In
Packet list
Packet bytes
String Options
Direction
Up
Help
Find
Cancel

By: ○ Display filter ○ Hex value ● String

Filter: pwd

Search In: ● Packet details

☐ Case sensitive

Character set: ASCII Unicode & Non-Unicode

Direction: ● Down

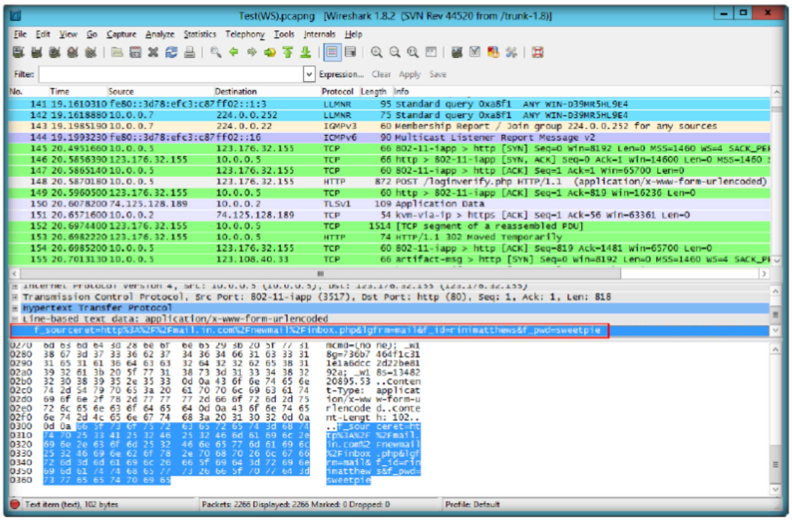
FIGURE 5.12: Wireshark – Selecting Options in Find Packet Window

Wireshark will not manipulate things on the network, it will only "measure" things from it. Wireshark doesn't send packets on the network or do other active things (except for name resolutions, but even that can be disabled).

TASK 3

Observe the Password

17. Wireshark will now display the sniffed password from the captured packets.



Test(WS).pcapng [Wireshark 1.8.2 (SVN Rev 44520 from /trunk-1.8)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.  Time       Source                Destination     Protocol Length Info
 141 19.1610310 fe80::3d78:efc3:c87 ff02::1:3       LLMNR     95 Standard query 0xa8f1  ANY WIN-D39MR5HL9E4
 142 19.1618880 10.0.0.7            224.0.0.252     LLMNR     75 Standard query 0xa8f1  ANY WIN-D39MR5HL9E4
 143 19.1985190 10.0.0.7            224.0.0.22      IGMPv3    60 Membership Report / Join group 224.0.0.252 for any sources
 144 19.1993230 fe80::3d78:efc3:c87 ff02::16        ICMPv6    90 Multicast Listener Report Message v2
 145 20.4951660 10.0.0.5            123.176.32.155  TCP       66 802-11-iapp > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PE
 146 20.5856390 123.176.32.155      10.0.0.5        TCP       66 http > 802-11-iapp [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 
 147 20.5865140 10.0.0.5            123.176.32.155  TCP       60 802-11-iapp > http [ACK] Seq=1 Ack=1 Win=65700 Len=0
 148 20.5870180 10.0.0.5            123.176.32.155  HTTP     872 POST /loginverify.php HTTP/1.1  (application/x-www-form-urlencoded)
 149 20.5960500 123.176.32.155      10.0.0.5        TCP       60 http > 802-11-iapp [ACK] Seq=1 Ack=819 Win=16236 Len=0
 150 20.6078200 74.125.128.189      10.0.0.2        TLSv1    109 Application Data
 151 20.6571600 10.0.0.2            74.125.128.189  TCP       54 kvm-via-ip > https [ACK] Seq=1 Ack=56 Win=63361 Len=0
 152 20.6974400 123.176.32.155      10.0.0.5        TCP     1514 [TCP segment of a reassembled PDU]
 153 20.6982220 123.176.32.155      10.0.0.5        HTTP      74 HTTP/1.1 302 Moved Temporarily
 154 20.6985200 10.0.0.5            123.176.32.155  TCP       60 802-11-iapp > http [ACK] Seq=819 Ack=1481 Win=65700 Len=0
 155 20.7013130 10.0.0.5            123.108.40.33   TCP       66 artifact-msg > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PE
```

```
⊞ Transmission Control Protocol, Src Port: 802-11-iapp (3517), Dst Port: http (80), Seq: 1, Ack: 1, Len: 818
⊞ Hypertext Transfer Protocol
⊟ Line-based text data: application/x-www-form-urlencoded
    f_sourceret=http%3A%2F%2Fmail.in.com%2Fnewmail%2Finbox.php&lgfrm=mail&f_id=rinimatthews&f_pwd=sweetpie
```

```
0270  6d 63 6d 64 3d 28 6e 6f  6e 65 29 3b 20 5f 77 31   mcmd=(no ne); _w1
0280  38 67 3d 37 33 36 62 37  34 36 34 66 31 63 33 31   8g=736b7 464f1c31
0290  31 65 31 61 36 64 63 63  32 64 32 32 62 65 38 31   1e1a6dcc 2d22be81
02a0  39 32 61 3b 20 5f 77 31  38 73 3d 31 33 34 38 32   92a; _w1 8s=13482
02b0  32 30 38 39 35 2e 35 33  0d 0a 43 6f 6e 74 65 6e   20895.53 ..Conten
02c0  74 2d 54 79 70 65 3a 20  61 70 70 6c 69 63 61 74   t-Type:  applicat
02d0  69 6f 6e 2f 78 2d 77 77  77 2d 66 6f 72 6d 2d 75   ion/x-ww w-form-u
02e0  72 6c 65 6e 63 6f 64 65  64 0d 0a 43 6f 6e 74 65   rlencode d..Conte
02f0  6e 74 2d 4c 65 6e 67 74  68 3a 20 31 30 32 0d 0a   nt-Lengt h: 102..
0300  0d 0a 66 5f 73 6f 75 72  63 65 72 65 74 3d 68 74   ..f_sour ceret=ht
0310  74 70 25 33 41 25 32 46  25 32 46 6d 61 69 6c 2e   tp%3A%2F %2Fmail.
0320  69 6e 2e 63 6f 6d 25 32  46 6e 65 77 6d 61 69 6c   in.com%2 Fnewmail
0330  25 32 46 69 6e 62 6f 78  2e 70 68 70 26 6c 67 66   %2Finbox .php&lgf
0340  72 6d 3d 6d 61 69 6c 26  66 5f 69 64 3d 72 69 6e   rm=mail& f_id=rin
0350  69 6d 61 74 74 68 65 77  73 26 66 5f 70 77 64 3d   imatthew s&f_pwd=
0360  73 77 65 65 74 70 69 65                            sweetpie
```

Text item (text), 102 bytes
Packets: 2266 Displayed: 2266 Marked: 0 Dropped: 0
Profile: Default

FIGURE 5.13: Wireshark – Sniffed Password in Captured Packet

Wireshark media types are supported depends on many things like the operating system you are using.

18. If you are working on **iLabs** environment, then use the **Test(WS)** sample captured file located at **D:\CEH-Tools\CEHv8 Module 08 Sniffing\Sniffing Tools\Wireshark\Wireshark Sample Capture files** to sniff the password.

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and "exposure" through public and free information.

Tool/Utility	Information Collected/Objectives Achieved
Wireshark	▪ Time ▪ Source ▪ Destination ▪ Protocol ▪ Length ▪ Info ▪ Internet Protocol ▪ TCP, Source Port Info ▪ User ID and Password

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Evaluate the protocols that are supported by Wireshark.
2. Determine the devices Wireshark uses to capture packets.

Internet Connection Required	
☑ **Yes**	☐ No
Platform Supported	
☑ **Classroom**	☐ iLabs

Lab

6

Performing Man-in-the-Middle Attack Using Cain & Abel

Cain &Abel is a password recovery tool that allows recovery of passwords by sniffing the network, cracking encrypted passwords.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

You have learned in the previous lab how you can get user name and password information using Wireshark. By merely capturing enough packets, attackers can extract the user name and password if the victim authenticates themselves in a public network especially into a website without an HTTPS connection. Once the password is hacked, an attacker can simply log into the victim's email account or use that password to log in to their PayPal and drain their bank account. They can even change the password for the email. Attackers can use Wireshark to decrypt the frames with the victim's password they already have.

As preventive measures an administrator in an organization should always advise employees not provide sensitive information in public networks without an HTTPS connection. VPN and SSH tunneling must be used to secure the network connection. As an expert **ethical hacker** and **penetration tester** you must have sound knowledge of sniffing, network protocols and their topology , TCP and UDP services, routing tables, **remote access** (SSH or VPN), authentication mechanism, and **encryption** techniques.

Another method through which you can gain user name and password information is by using Cain & Abel to perform a man-in-the-middle attack.

Lab Objectives

The objective of this lab to accomplish the following information regarding the target organization that includes, but is not limited to:

- Sniff network traffic and perform ARP poisoning
- Launch a man-in-the-middle attack
- Sniff the network for the password

Lab Environment

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 08 Sniffing

To carry-out the lab, you need:

- **Cain & Abel** located at **D:\CEH-Tools\CEHv8 Module 08 Sniffing\ARP Poisoning Tools\Cain & Abel**
- You can also download the latest version of **Cain & Abel** from http://www.oxid.it
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- A computer running **Windows Server 2012** as host machine
- **Windows 8** running on virtual machine as attacker machine
- **Windows 2008 Server** running on virtual machine as the victim machine
- A web browser with Internet connection
- Double-click **ca_setup.exe** and follow the wizard-driven installation steps to install Cain & Abel
- Administrative privileges to run tools

Lab Duration

Time: 20 Minutes

Overview of Man-In-The-Middle Attack

You can download Cain & Abel from http://www.oxid.it.

A man-in-the-middle attack (MITM) is a form of **active eavesdropping** in which the attacker makes **independent** connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a **private connection**, when in fact the entire conversation is **controlled** by the attacker.

Man-in-the-middle attacks come in many **variations** and can be carried out on a **switched** LAN.

Lab Tasks

TASK 1

Man-In-The-Middle Attack

1. Launch your **Windows 2008 Server** virtual machine (**Victim Machine**).
2. Launch your **Windows 8** virtual machine (**Attacker Machine**).
3. On the host machine (Windows Server 2012), launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

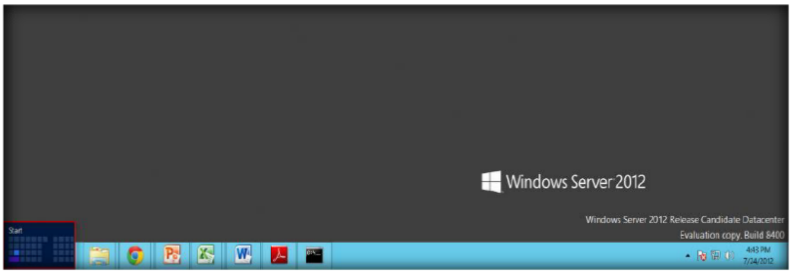

Windows Server 2012
Windows Server 2012 Release Candidate Datacenter
Evaluation copy. Build 8400
Start

FIGURE 6.1: Windows Server 2012 – Desktop view

Man in the Middle attacks has the potential to eavesdrop on a switched LAN to sniff for clear-text data (McClure, Scambray). It can also be used for substitution attacks that can actively manipulate data.

4. Click **Cain** in the **Start** menu to launch Cain& Abel.

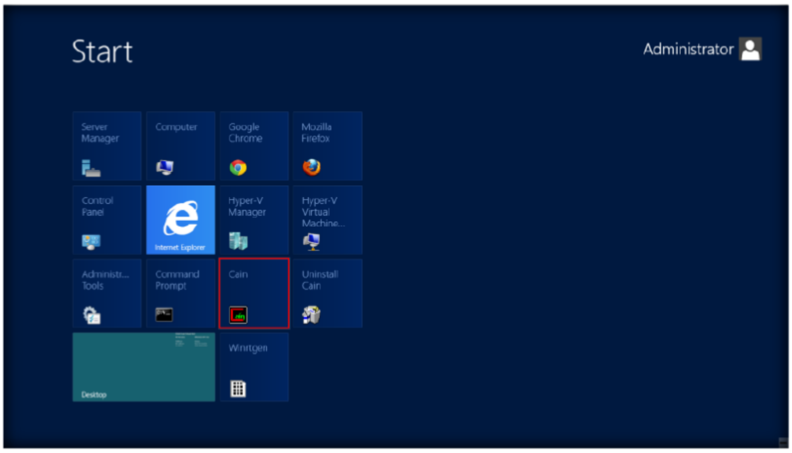
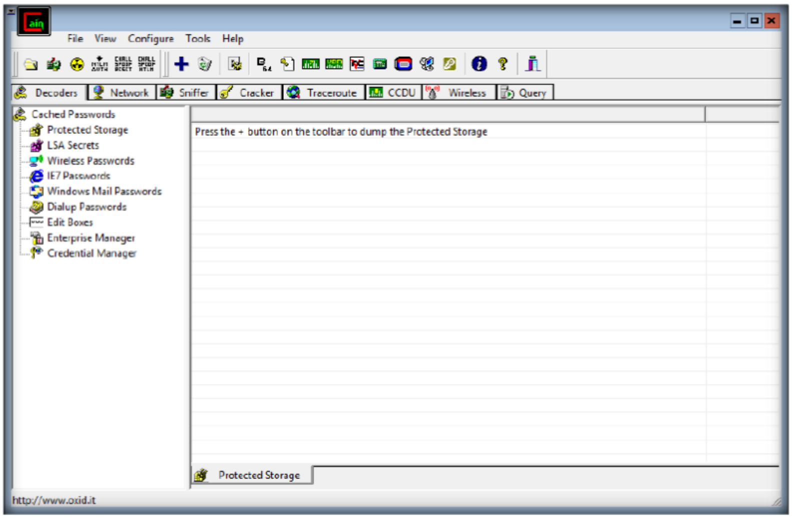

Start
Administrator
Server Manager
Computer
Google Chrome
Mozilla Firefox
Control Panel
Internet Explorer
Hyper-V Manager
Hyper-V Virtual Machine...
Administr... Tools
Command Prompt
Cain
Uninstall Cain
Desktop
Winrtgen

FIGURE 6.2: Windows Server 2012 – Desktop view

Cain & Abel covers some security aspects/weakness intrinsic of protocol's standards, authentication methods and caching mechanisms.

5. The main window of Cain & Abel appears.


File View Configure Tools Help
Decoders
Network
Sniffer
Cracker
Traceroute
CCDU
Wireless
Query
Cached Passwords
Protected Storage
LSA Secrets
Wireless Passwords
IE7 Passwords
Windows Mail Passwords
Dialup Passwords
Edit Boxes
Enterprise Manager
Credential Manager
Protected Storage
http://www.oxid.it

Press the + button on the toolbar to dump the Protected Storage

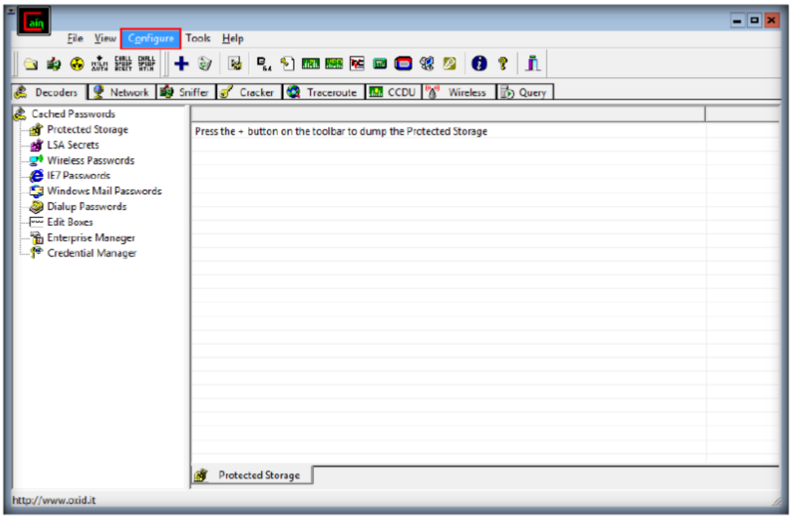
FIGURE 6.3: Cain & Abel Main Window

Replay attacks can also be used to resend a sniffed password hash to authenticate an unauthorized user.

6. When you first open Cain & Abel, you will notice a series of tabs near the top of the window.

7. To configure the **Ethernet card**, click **Configure** from the menu bar.

APR-SSH1 can capture and decrypt SSH version 1 session that are then saved toa text file. APR-HTTPS can intercept and forge digital certificates on the fly but becauses trusted authority does not sign these certificates a warning message will be displayed to the end user.


File
View
Configure
Tools
Help
Decoders
Network
Sniffer
Cracker
Traceroute
CCDU
Wireless
Query
Cached Passwords
Protected Storage
LSA Secrets
Wireless Passwords
IE7 Passwords
Windows Mail Passwords
Dialup Passwords
Edit Boxes
Enterprise Manager
Credential Manager
Protected Storage
http://www.oxid.it

Press the + button on the toolbar to dump the Protected Storage

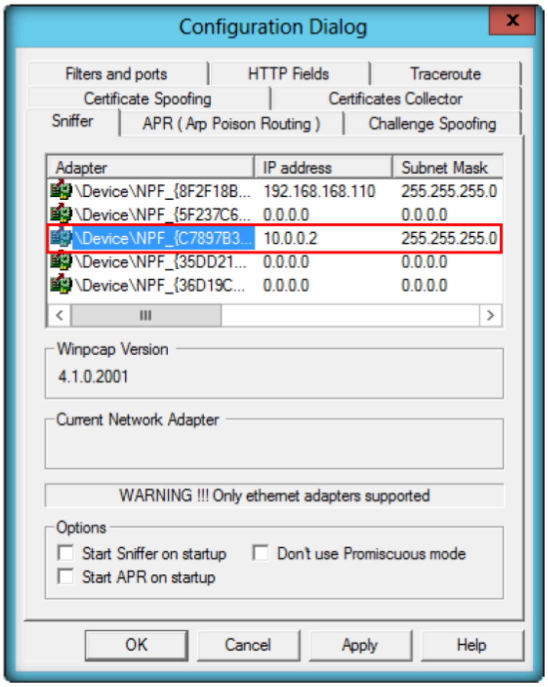
FIGURE 6.4: Cain & Abel Configuration Option

FIGURE 6.4: Cain & Abel Configuration Option

8. The **Configuration Dialog** window appears.
9. The **Configuration Dialog** window consists of several tabs. Click the **Sniffer** tab to select the sniffing adapter.
10. Select **Adapter** and click **Apply** and then **OK**.

For IP and MAC spoofing you have to choose addresses that are not already present on the network. By default Cain uses the spoofed MAC "001122334455" for two reasons: first that address can be easily identified for troubleshooting and second it is not supposed to exist in your network.

Note: You cannot have on the same Layer-2 network two or more Cain machines using APR's MAC spoofing and the same Spoofed MAC address.


Configuration Dialog
X
Filters and ports
HTTP Fields
Traceroute
Certificate Spoofing
Certificates Collector
Sniffer
APR (Arp Poison Routing)
Challenge Spoofing
OK
Cancel
Apply
Help

Adapter	IP address	Subnet Mask
\Device\NPF_{8F2F18B...	192.168.168.110	255.255.255.0
\Device\NPF_{5F237C6...	0.0.0.0	0.0.0.0
\Device\NPF_{C7897B3...	10.0.0.2	255.255.255.0
\Device\NPF_{35DD21...	0.0.0.0	0.0.0.0
\Device\NPF_{36D19C...	0.0.0.0	0.0.0.0

Winpcap Version
4.1.0.2001

Current Network Adapter

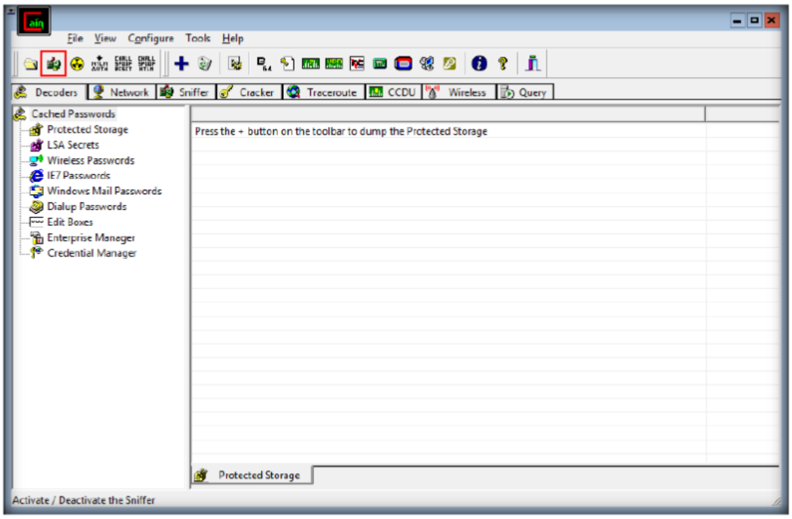
WARNING !!! Only ethernet adapters supported

Options
☐ Start Sniffer on startup
☐ Don't use Promiscuous mode
☐ Start APR on startup

FIGURE 6.5: Cain & Abel Configuration Dialog Window

11. Click the **Start/Stop Sniffer** icon on the toolbar.

The most crucial item in that list is the radioactive hazard APR. It is in this window that we select our victim(s).


File
View
Configure
Tools
Help
Decoders
Network
Sniffer
Cracker
Traceroute
CCDU
Wireless
Query
Cached Passwords
Protected Storage
LSA Secrets
Wireless Passwords
IE7 Passwords
Windows Mail Passwords
Dialup Passwords
Edit Boxes
Enterprise Manager
Credential Manager
Protected Storage

Press the + button on the toolbar to dump the Protected Storage

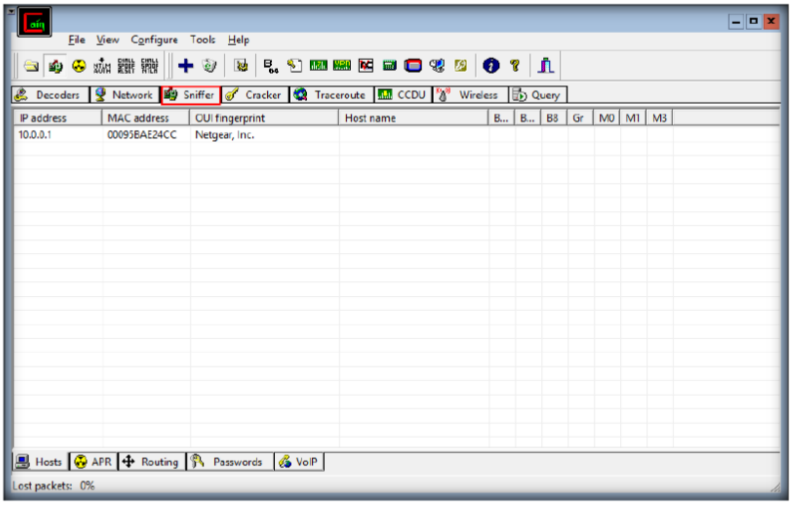
Activate / Deactivate the Sniffer

FIGURE 6.6: Cain & Abel Configuration Dialog Window

FIGURE 6.6: Cain & Abel Configuration Dialog Window

Note: If you get Cain Warning pop-up, click **OK**.

12. Now click the **Sniffer** tab.


File
View
Configure
Tools
Help
Decoders
Network
Sniffer
Cracker
Traceroute
CCDU
Wireless
Query
Hosts
APR
Routing
Passwords
VoIP

IP address	MAC address	OUI fingerprint	Host name	B...	B...	B8	Gr	M0	M1	M3
10.0.0.1	00095BAE24CC	Netgear, Inc.								

Lost packets: 0%

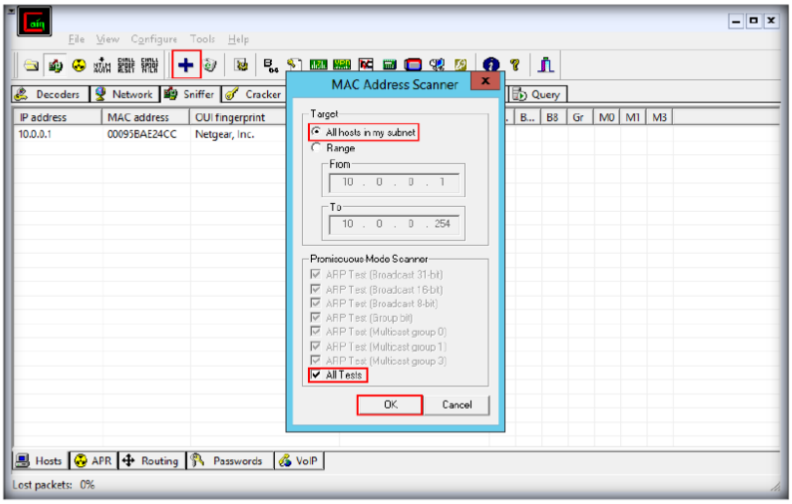
FIGURE 6.7: Sniffer tab

Be warned that there is the possibility that you will cause damages and/or loss of data using this software and that in no events shall the author be liable for such damages or loss of data.

13. Click the **Plus** (**+**) icon or right-click in the window and select **Scan MAC Addresses** to scan the network for hosts.

14. The **MAC Address Scanner** window appears. Select **All hosts in my subnet** and check the **All Tests** check box. Click **OK**.

APR-RDP can capture and decrypt Microsoft's Remote Desktop Protocol as well.


File
View
Configure
Tools
Help
Decoders
Network
Sniffer
Cracker
Query
Hosts
APR
Routing
Passwords
VoIP
Lost packets: 0%

IP address	MAC address	OUI fingerprint
10.0.0.1	00095BAE24CC	Netgear, Inc.

MAC Address Scanner

Target
● All hosts in my subnet
○ Range
From 10 . 0 . 0 . 1
To 10 . 0 . 0 . 254

Promiscuous Mode Scanner
☑ ARP Test (Broadcast 31-bit)
☑ ARP Test (Broadcast 16-bit)
☑ ARP Test (Broadcast 8-bit)
☑ ARP Test (Group bit)
☑ ARP Test (Multicast group 0)
☑ ARP Test (Multicast group 1)
☑ ARP Test (Multicast group 3)
☑ All Tests

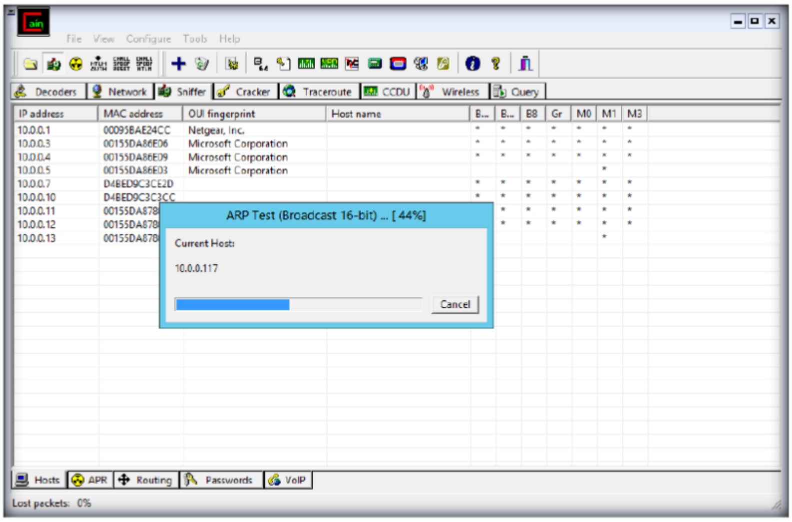
OK
Cancel

FIGURE 6.8: Cain & Abel – MAC Address Scanner Window

FIGURE 6.8: Cain & Abel – MAC Address Scanner Window

15. Cain & Abel starts scanning for MAC addresses and lists all found MAC address.

Speeding up packet capture speed by wireless packet injection


File
View
Configure
Tools
Help
Decoders
Network
Sniffer
Cracker
Traceroute
CCDU
Wireless
Query
Hosts
APR
Routing
Passwords
VoIP
Lost packets: 0%

IP address	MAC address	OUI fingerprint	Host name	B...	B...	B8	Gr	M0	M1	M3
10.0.0.1	00095BAE24CC	Netgear, Inc.		*	*	*	*	*	*	*
10.0.0.3	00155DA86E06	Microsoft Corporation		*	*	*	*	*	*	*
10.0.0.4	00155DA86E09	Microsoft Corporation		*	*	*	*	*	*	*
10.0.0.5	00155DA86E03	Microsoft Corporation							*	
10.0.0.7	D4BED9C3CE2D			*	*	*	*	*	*	*
10.0.0.10	D4BED9C3C3CC			*	*	*	*	*	*	*
10.0.0.11	00155DA878				*	*	*	*	*	*
10.0.0.12	00155DA878				*	*	*	*	*	*
10.0.0.13	00155DA878								*	

ARP Test (Broadcast 16-bit) ... [44%]

Current Host:

10.0.0.117

Note that Cain & Abel program does not exploit any software vulnerabilities or bugs that could not be fixed with little effort.

FIGURE 6.9: Cain & Abel – Scanning MAC Addresses Window

16. After scanning is **completed**, a list of detected **MAC addresses** is displayed.
17. Click the **APR** tab at the bottom of the main window.

APR state Half-Routing means that APR is routing the traffic correctly but only in one direction (ex: Client->Server or Server->Client). This can happen if one of the two hosts cannot be poisoned or if asymmetric routing is used on the LAN. In this state the sniffer loses all packets of an entire direction so it cannot grab authentications that use a challenge-response mechanism.

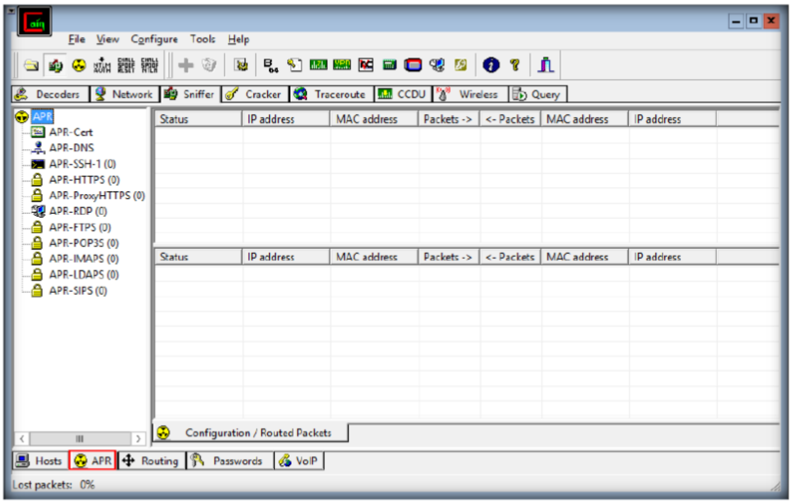

File
View
Configure
Tools
Help
Decoders
Network
Sniffer
Cracker
Traceroute
CCDU
Wireless
Query
APR
APR-Cert
APR-DNS
APR-SSH-1 (0)
APR-HTTPS (0)
APR-ProxyHTTPS (0)
APR-RDP (0)
APR-FTPS (0)
APR-POP3S (0)
APR-IMAPS (0)
APR-LDAPS (0)
APR-SIPS (0)
Status
IP address
MAC address
Packets ->
<- Packets
MAC address
IP address
Configuration / Routed Packets
Hosts
APR
Routing
Passwords
VoIP
Lost packets: 0%

FIGURE 6.10: Cain & Abel ARP Tab

FIGURE 6.10: Cain & Abel ARP Tab

18. Click anywhere in the **Configuration/Routed Packets** window of APR to activate the **Plus** icon.

APR state Full-Routing means that the IP traffic between two hosts has been completely hijacked and APR is working in FULL-DUPLEX. (ex: Server<->Client). The sniffer will grab authentication information accordingly to the sniffer filters set.

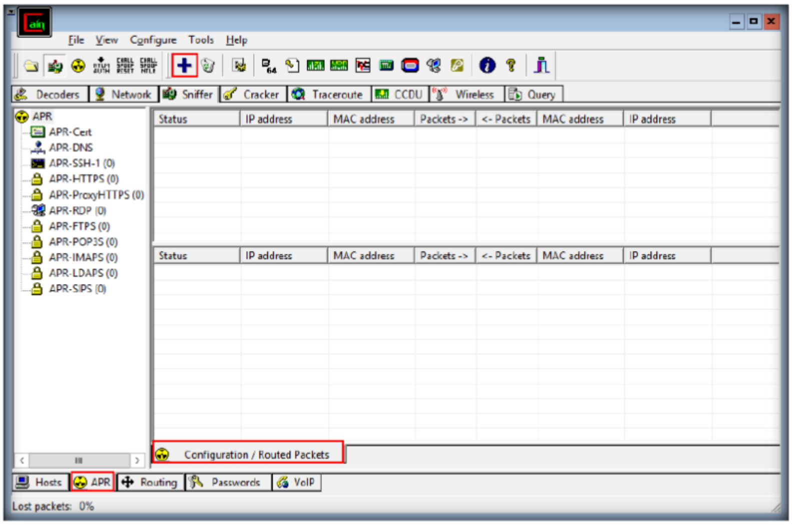
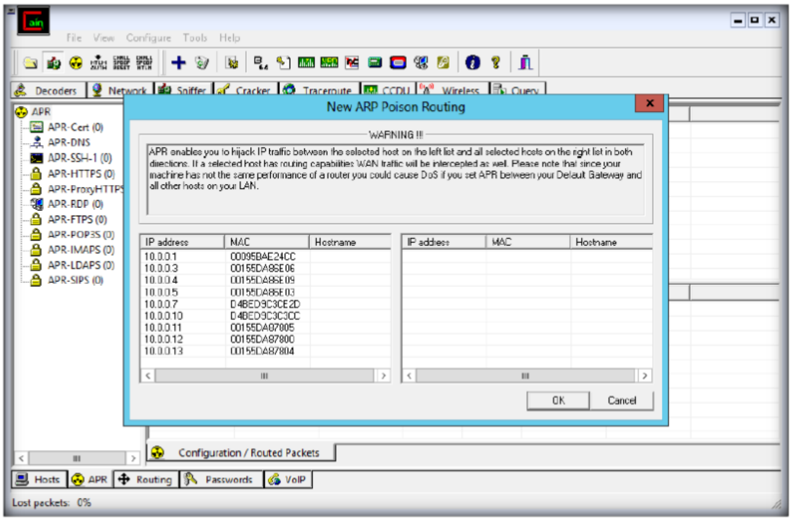

File
View
Configure
Tools
Help
Decoders
Network
Sniffer
Cracker
Traceroute
CCDU
Wireless
Query
APR
APR-Cert
APR-DNS
APR-SSH-1 (0)
APR-HTTPS (0)
APR-ProxyHTTPS (0)
APR-RDP (0)
APR-FTPS (0)
APR-POP3S (0)
APR-IMAPS (0)
APR-LDAPS (0)
APR-SIPS (0)
Status
IP address
MAC address
Packets ->
<- Packets
MAC address
IP address
Configuration / Routed Packets
Hosts
APR
Routing
Passwords
VoIP
Lost packets: 0%

FIGURE 6.11: Cain & Abel ARP Tab

19. Click the Plus (**+**) icon; the **New ARP Poison Routing** window opens from which you can add the IPs to listen to traffic.


Cain
File View Configure Tools Help
Decoders
Network
Sniffer
Cracker
Traceroute
CCDU
Wireless
Query
APR
APR-Cert (0)
APR-DNS
APR-SSH-1 (0)
APR-HTTPS (0)
APR-ProxyHTTPS
APR-RDP (0)
APR-FTPS (0)
APR-POP3S (0)
APR-IMAPS (0)
APR-LDAPS (0)
APR-SIPS (0)
New ARP Poison Routing
WARNING !!!
OK
Cancel
Configuration / Routed Packets
Hosts
APR
Routing
Passwords
VoIP
Lost packets: 0%

APR enables you to hijack IP traffic between the selected host on the left list and all selected hosts on the right list in both directions. If a selected host has routing capabilities WAN traffic will be intercepted as well. Please note that since your machine has not the same performance of a router you could cause DoS if you set APR between your Default Gateway and all other hosts on your LAN.

IP address	MAC	Hostname
10.0.0.1	00095BAE24CC	
10.0.0.3	00155DA86E06	
10.0.0.4	00155DA86E09	
10.0.0.5	00155DA86E03	
10.0.0.7	D4BED9C3CE2D	
10.0.0.10	D4BED9C3C3CC	
10.0.0.11	00155DA87805	
10.0.0.12	00155DA87800	
10.0.0.13	00155DA87804	

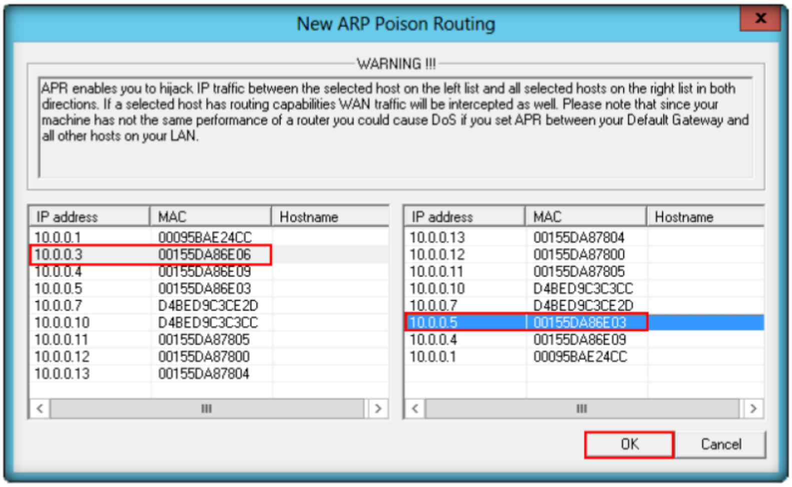
IP address	MAC	Hostname

The Protected Store is a storage facility provided as part of Microsoft CryptoAPI. It's primarily use is to securely store private keys that have been issued to a user.

FIGURE 6.12: Cain & Abel ARP Tab

FIGURE 6.12: Cain & Abel ARP Tab

20. To monitor the traffic between two computers, select **10.0.0.3** (Windows 8 virtual machine) and **10.0.0.5** (Windows 2008 Server virtual machine). Click **OK**.


New ARP Poison Routing
WARNING !!!
OK
Cancel

APR enables you to hijack IP traffic between the selected host on the left list and all selected hosts on the right list in both directions. If a selected host has routing capabilities WAN traffic will be intercepted as well. Please note that since your machine has not the same performance of a router you could cause DoS if you set APR between your Default Gateway and all other hosts on your LAN.

IP address	MAC	Hostname
10.0.0.1	00095BAE24CC	
10.0.0.3	00155DA86E06	
10.0.0.4	00155DA86E09	
10.0.0.5	00155DA86E03	
10.0.0.7	D4BED9C3CE2D	
10.0.0.10	D4BED9C3C3CC	
10.0.0.11	00155DA87805	
10.0.0.12	00155DA87800	
10.0.0.13	00155DA87804	

IP address	MAC	Hostname
10.0.0.13	00155DA87804	
10.0.0.12	00155DA87800	
10.0.0.11	00155DA87805	
10.0.0.10	D4BED9C3C3CC	
10.0.0.7	D4BED9C3CE2D	
10.0.0.5	00155DA86E03	
10.0.0.4	00155DA86E09	
10.0.0.1	00095BAE24CC	

All of the information in the Protected Store is encrypted, using a key that is derived from the user's logon password. Access to the information is tightly regulated so that only the owner of the material can access it

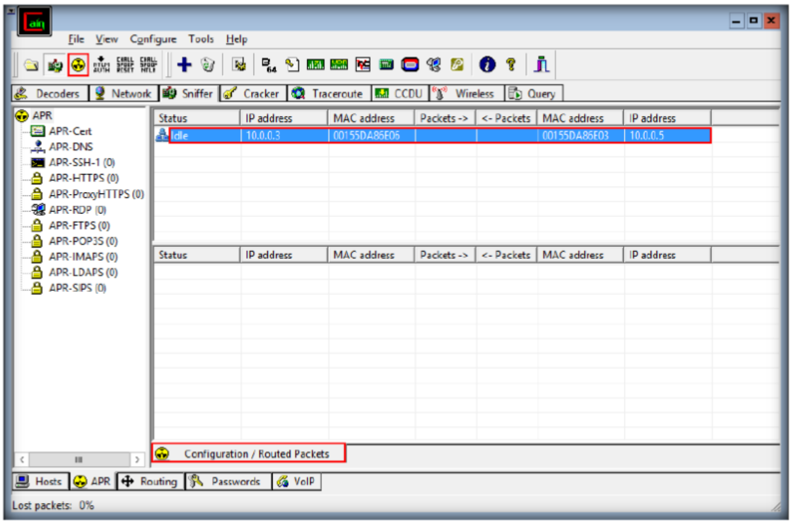
FIGURE 6.13: Cain & Abel ARP Tab

FIGURE 6.13: Cain & Abel ARP Tab

21. Select the added IP address in the **Configuration/Routed** packets and click the **Start/Stop APR** icon.

Note: If the Couldn't bind HTTPS acceptor socket pop-up appears, click **OK**.

📖 Many Windows applications use this feature; Internet Explorer, Outlook and Outlook Express for example store user names and passwords using this service.


File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
APR
APR-Cert
APR-DNS
APR-SSH-1 (0)
APR-HTTPS (0)
APR-ProxyHTTPS (0)
APR-RDP (0)
APR-FTPS (0)
APR-POP3S (0)
APR-IMAPS (0)
APR-LDAPS (0)
APR-SIPS (0)
Configuration / Routed Packets
Hosts APR Routing Passwords VoIP
Lost packets: 0%

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Idle	10.0.0.3	00155DA86E06			00155DA86E03	10.0.0.5

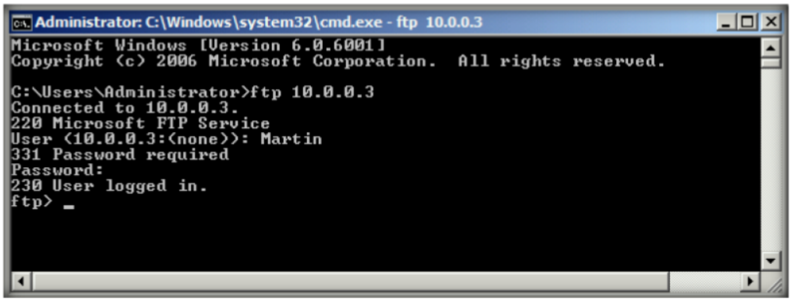
FIGURE 6.14: Cain & Abel ARP Poisoning

FIGURE 6.14: Cain & Abel ARP Poisoning

22. Now launch the command prompt in Windows 2008 Server and type **ftp 10.0.0.3** (IP address of Windows 8 machine) and press **Enter**.

23. When prompted for Username type "**Martin**" and press **Enter** and for password type "**apple**" and press **Enter**.

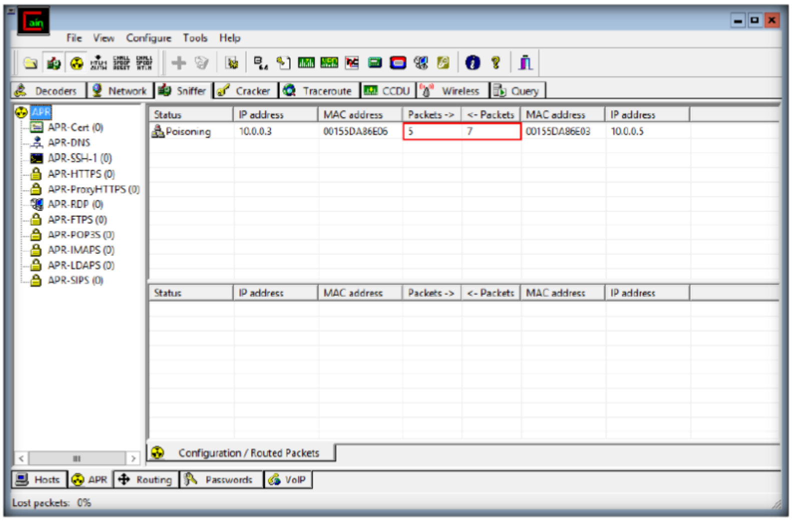
📖 There is also another set used for credentials that should persist on the local machine only and cannot be used in roaming profiles, this is called "Local Credential Set" and it refers to the file: \Documents and Settings\%Username%\Local Settings\Application Data\Microsoft\Credentials\%UserSID%\Credentials


Administrator: C:\Windows\system32\cmd.exe - ftp 10.0.0.3

```
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator>ftp 10.0.0.3
Connected to 10.0.0.3.
220 Microsoft FTP Service
User (10.0.0.3:(none)): Martin
331 Password required
Password:
230 User logged in.
ftp> _
```

FIGURE 6.15: Start ftp://10.0.0.3

24. Now, on the host machine, observe the tool listing some packets exchange.


File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
APR
APR-Cert (0)
APR-DNS
APR-SSH-1 (0)
APR-HTTPS (0)
APR-ProxyHTTPS (0)
APR-RDP (0)
APR-FTPS (0)
APR-POP3S (0)
APR-IMAPS (0)
APR-LDAPS (0)
APR-SIPS (0)
Configuration / Routed Packets
Hosts APR Routing Passwords VoIP
Lost packets: 0%

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Poisoning	10.0.0.3	00155DA86E06	5	7	00155DA86E03	10.0.0.5

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address

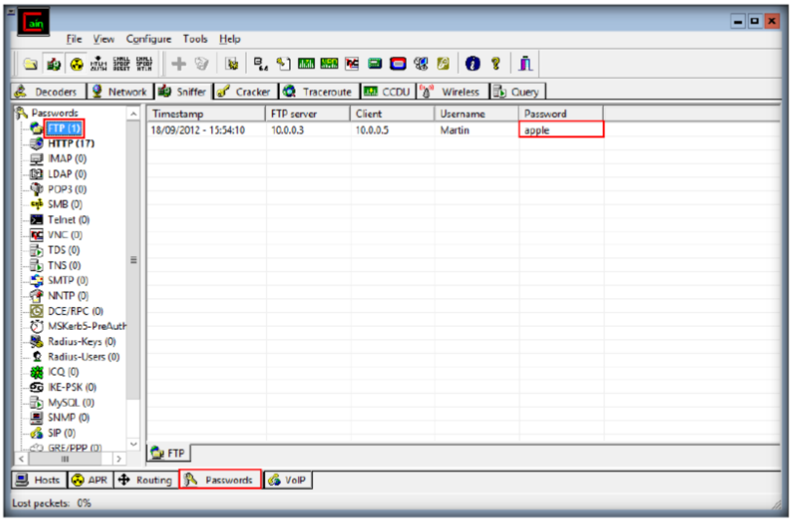
FIGURE 6.16: Sniffer window with more packets exchanged

FIGURE 6.16: Sniffer window with more packets exchanged

Credentials are stored in the registry under the key HKEY_CURRENT_USER \Software\Microsoft\Protected Storage System Provider\

25. Click the **Passwords** tab as shown in the following screenshot to view the sniffed password for **ftp 10.0.0.3**.

This set of credentials is stored in the file \Documents and Settings\%Username%\Application Data\Microsoft\Credentials \%UserSID%\Credentials


File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
Passwords
FTP (1)
HTTP (17)
IMAP (0)
LDAP (0)
POP3 (0)
SMB (0)
Telnet (0)
VNC (0)
TDS (0)
TNS (0)
SMTP (0)
NNTP (0)
DCE/RPC (0)
MSKerb5-PreAuth
Radius-Keys (0)
Radius-Users (0)
ICQ (0)
IKE-PSK (0)
MySQL (0)
SNMP (0)
SIP (0)
GRE/PPP (0)
FTP
Hosts APR Routing Passwords VoIP
Lost packets: 0%

Timestamp	FTP server	Client	Username	Password
18/09/2012 - 15:54:10	10.0.0.3	10.0.0.5	Martin	apple

FIGURE 6.17: Sniffer window with more packets exchanged

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and "exposure" through public and free information.

Tool/Utility	Information Collected/Objectives Achieved
Cain & Abel	**IP Address** – 10.0.0.3 **MAC Address** – 00155DA86E06 **Packets Sent** – 5 **Packets Received** – 7 **FTP Server** – 10.0.0.3 **Username** – Martin **Password** – apple

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Determine how you can defend against ARP cache poisoning in a network.
2. How can you easily find the password captured in an EDP MITM attack using only Notepad or some other text editor?
3. How can one protect a Windows Server against RDP MITM attacks?

Internet Connection Required	
☑ **Yes**	☐ No
Platform Supported	
☑ **Classroom**	☑ iLabs

Lab

7

Detecting ARP Attacks with the XArp Tool

XArp is a security application that uses advanced techniques to detect ARP-based attacks.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

You have already learned in the previous lab to capture user name and password information using Cain & Abel. Similarly, attackers, too, can sniff the username and password of a user. Once attackers have a user name and password, they can simply gain access to a network's database and perform illegitimate activities. If that account has administrator permissions, attackers can disable firewalls and load fatal viruses and worms on the computer and spread that onto the network. They can also perform different types of attacks such as denial-of-service attacks, spoofing, buffer overflow, heap overflow, etc.

When using a wireless connection, as an administrator you must use the strongest security supported by your wireless devices and also advise other employees to use a strong password. The passwords must be changed weekly or monthly.

Another method attackers can implement is ARP attacks through which they can snoop or manipulate all your data passing over the network. This includes documents, emails, and VoiceIP conversations. ARP attacks go undetected by firewalls; hence, in this lab you will be guided to use the XArp tool, which provides advanced techniques to detect ARP attacks to prevent your data.

Lab Objectives

The objective of this lab to accomplish the following regarding the target organization that includes, but is not limited to:

- To detect ARP attacks

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 08 Sniffing

Lab Environment

To carry-out the lab, you need:

- **XArp** is located at **D:\CEH-Tools\CEHv8 Module 08 Sniffing\ARP Spoofing Detection Tools\XArp**
- You can also download the latest version of **XArp** from http://www.chrismc.de/development/xarp/index.html
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- A computer running Windows Server 2012 as host machine
- Double-click **xarp-2.2.2-win.exe** and follow the wizard-driven installation steps to install **XArp**
- Administrative privileges to run tools

Lab Duration

Time: 10 Minutes

Overview of XArp

XArp helps users to detect ARP attacks and keep their data private. Administrators can use XArp to monitor whole subnets for ARP attacks. Different security levels and fine-tuning possibilities allow normal and power users to efficiently use XArp to detect ARP attacks.

Lab Tasks

TASK 1

Launching the XArp tool

1. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

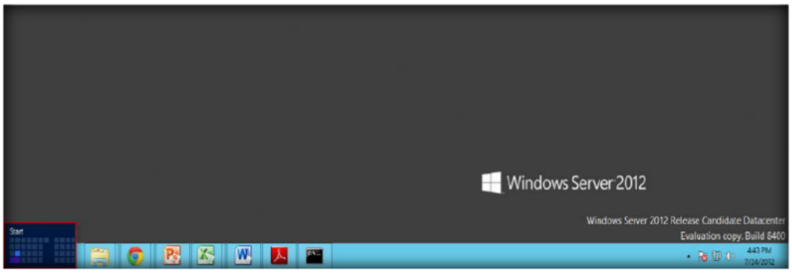

Start
Windows Server 2012
Windows Server 2012 Release Candidate Datacenter
Evaluation copy. Build 8400
4:43 PM
7/24/2012

FIGURE 7.1: Windows Server 2012 – Desktop view

2. Click **XArp** in the **Start** menu to launch the XArp tool.

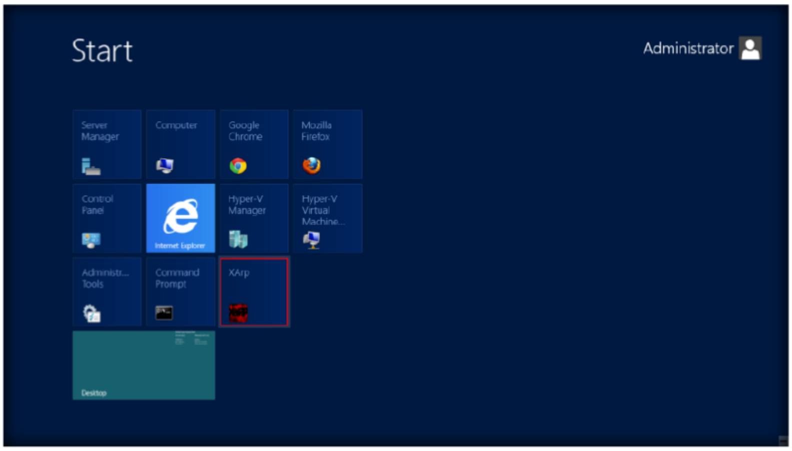
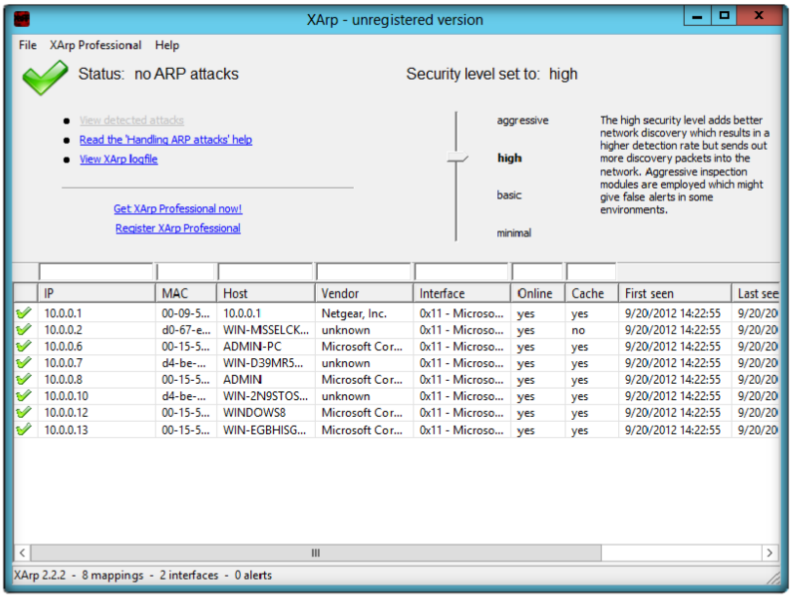

Start
Administrator
Server Manager
Computer
Google Chrome
Mozilla Firefox
Control Panel
Internet Explorer
Hyper-V Manager
Hyper-V Virtual Machine...
Administr... Tools
Command Prompt
XArp
Desktop

FIGURE 7.2: Windows Server 2012 – Apps

Address Resolution Protocol (ARP) poisoning is a type of attack where the Media Access Control (MAC) address is changed by the attacker.

3. The main Window of XArp appears with a list of IPs, MAC addresses, and other information for machines in the network.


XArp - unregistered version
File
XArp Professional
Help
View detected attacks
Read the 'Handling ARP attacks' help
View XArp logfile
Get XArp Professional now!
Register XArp Professional
aggressive
high
basic
minimal

Status: no ARP attacks

Security level set to: high

The high security level adds better network discovery which results in a higher detection rate but sends out more discovery packets into the network. Aggressive inspection modules are employed which might give false alerts in some environments.

	IP	MAC	Host	Vendor	Interface	Online	Cache	First seen	Last see
✓	10.0.0.1	00-09-5...	10.0.0.1	Netgear, Inc.	0x11 - Microso...	yes	yes	9/20/2012 14:22:55	9/20/20
✓	10.0.0.2	d0-67-e...	WIN-MSSELCK...	unknown	0x11 - Microso...	yes	no	9/20/2012 14:22:55	9/20/20
✓	10.0.0.6	00-15-5...	ADMIN-PC	Microsoft Cor...	0x11 - Microso...	yes	yes	9/20/2012 14:22:55	9/20/20
✓	10.0.0.7	d4-be-...	WIN-D39MR5...	unknown	0x11 - Microso...	yes	yes	9/20/2012 14:22:55	9/20/20
✓	10.0.0.8	00-15-5...	ADMIN	Microsoft Cor...	0x11 - Microso...	yes	yes	9/20/2012 14:22:55	9/20/20
✓	10.0.0.10	d4-be-...	WIN-2N9STOS...	unknown	0x11 - Microso...	yes	yes	9/20/2012 14:22:55	9/20/20
✓	10.0.0.12	00-15-5...	WINDOWS8	Microsoft Cor...	0x11 - Microso...	yes	yes	9/20/2012 14:22:55	9/20/20
✓	10.0.0.13	00-15-5...	WIN-EGBHISG...	Microsoft Cor...	0x11 - Microso...	yes	yes	9/20/2012 14:22:55	9/20/20

XArp 2.2.2 - 8 mappings - 2 interfaces - 0 alerts

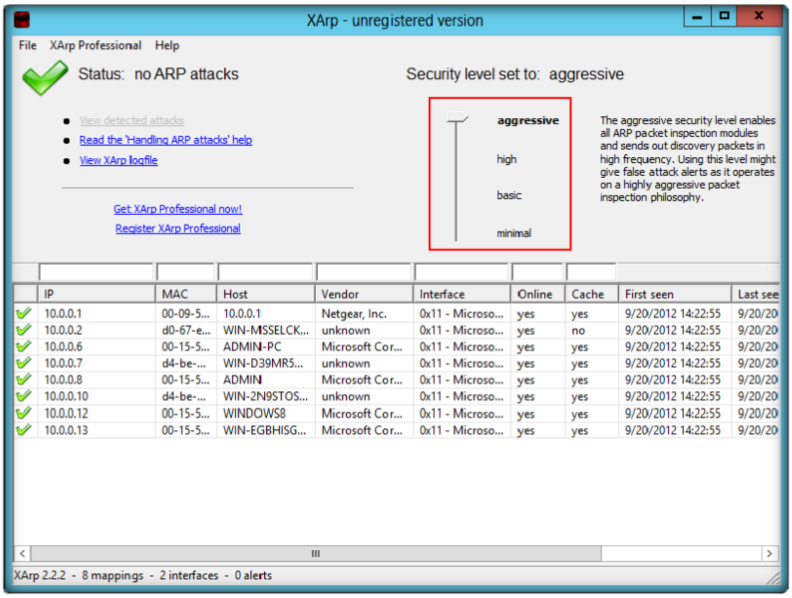
FIGURE 7.3: XArp status when security level set to high

A MAC address is a unique identifier for network nodes on a LAN. MAC addresses are associated to network adapter that connects devices to networks. The MAC address is critical to locating networked hardware devices because it ensures that data packets go to the correct place. ARP tables, or cache, are used to correlate network devices' IP addresses to their MAC addresses.

4. On the host machine, XArp displays no ARP attacks.

Note: If you observe the same results, log in to a virtual machine and run Cain & Abel to initiate ARP poisoning to the host machine.

5. By default the security level is set to high. Set the **Security level** to **aggressive** on the **XArp** screen.



XArp - unregistered version

Status: no ARP attacks

Security level set to: aggressive

View detected attacks
Read the 'Handling ARP attacks' help
View XArp logfile
Get XArp Professional now!
Register XArp Professional
aggressive
high
basic
minimal

The aggressive security level enables all ARP packet inspection modules and sends out discovery packets in high frequency. Using this level might give false attack alerts as it operates on a highly aggressive packet inspection philosophy.

	IP	MAC	Host	Vendor	Interface	Online	Cache	First seen	Last see
✓	10.0.0.1	00-09-5...	10.0.0.1	Netgear, Inc.	0x11 - Microso...	yes	yes	9/20/2012 14:22:55	9/20/20
✓	10.0.0.2	d0-67-e...	WIN-MSSELCK...	unknown	0x11 - Microso...	yes	no	9/20/2012 14:22:55	9/20/20
✓	10.0.0.6	00-15-5...	ADMIN-PC	Microsoft Cor...	0x11 - Microso...	yes	yes	9/20/2012 14:22:55	9/20/20
✓	10.0.0.7	d4-be-...	WIN-D39MR5...	unknown	0x11 - Microso...	yes	yes	9/20/2012 14:22:55	9/20/20
✓	10.0.0.8	00-15-5...	ADMIN	Microsoft Cor...	0x11 - Microso...	yes	yes	9/20/2012 14:22:55	9/20/20
✓	10.0.0.10	d4-be-...	WIN-2N9STOS...	unknown	0x11 - Microso...	yes	yes	9/20/2012 14:22:55	9/20/20
✓	10.0.0.12	00-15-5...	WINDOWS8	Microsoft Cor...	0x11 - Microso...	yes	yes	9/20/2012 14:22:55	9/20/20
✓	10.0.0.13	00-15-5...	WIN-EGBHISG...	Microsoft Cor...	0x11 - Microso...	yes	yes	9/20/2012 14:22:55	9/20/20

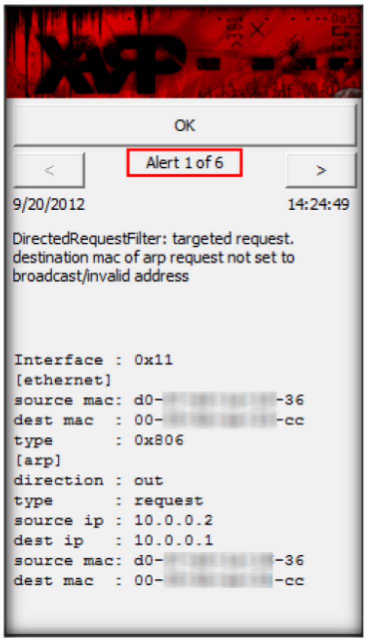
XArp 2.2.2 - 8 mappings - 2 interfaces - 0 alerts

FIGURE 7.4: XArp status when security level set to aggressive

🗁 An attacker can alter the MAC address of the device that is used to connect the network to Internet and can disable access to the web and other external networks.

6. Log in to Windows 2008 Server, and run Cain & Abel to initiate an ARP attack on a Windows 2012 host machine.

7. The XArp pop-up appears displaying the alerts.



9/20/2012 14:24:49

DirectedRequestFilter: targeted request. destination mac of arp request not set to broadcast/invalid address

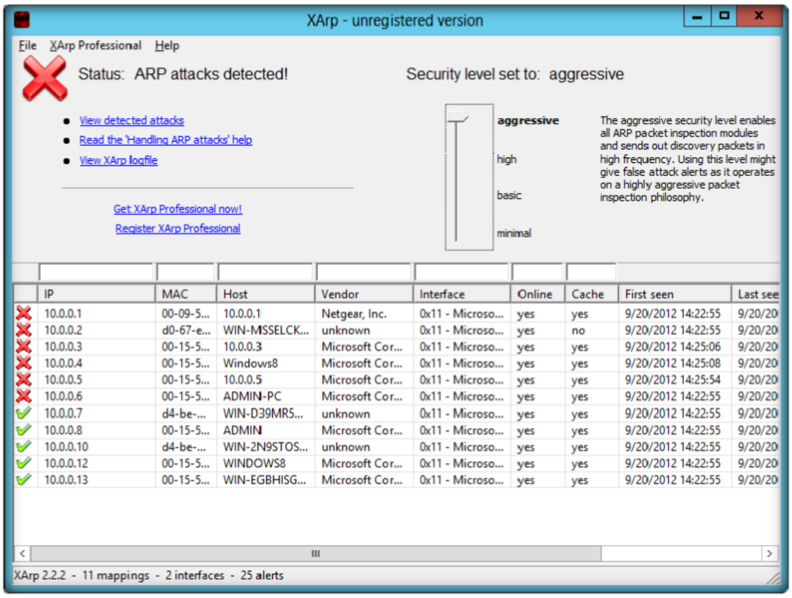
```
Interface : 0x11
[ethernet]
source mac: d0-[redacted]-36
dest mac  : 00-[redacted]-cc
type      : 0x806
[arp]
direction : out
type      : request
source ip : 10.0.0.2
dest ip   : 10.0.0.1
source mac: d0-[redacted]-36
dest mac  : 00-[redacted]-cc
```

FIGURE 7.5: XArp displaying Alerts

🗁 XArp allows alert filtering for excluding specific hosts. Another feature includes settings for alerting intensity and how the alerts are presented. Also allows sending alerts through email and detailed alerting configuration.

8. Now, the XArp **Status** changes to **ARP attacks detected**.

The simplest form of certification is the use of static, read-only entries for critical services in the ARP cache of a host. This only prevents simple attacks and does not scale on a large network, since the mapping has to be set for each pair of machines resulting in (n*n) ARP caches that have to be configured. AntiARP also provides Windows-based spoofing prevention at the kernel level.



Status: ARP attacks detected!

Security level set to: aggressive

- View detected attacks
- Read the 'Handling ARP attacks' help
- View XArp logfile

Get XArp Professional now!

Register XArp Professional

The aggressive security level enables all ARP packet inspection modules and sends out discovery packets in high frequency. Using this level might give false attack alerts as it operates on a highly aggressive packet inspection philosophy.

	IP	MAC	Host	Vendor	Interface	Online	Cache	First seen	Last see
✗	10.0.0.1	00-09-5...	10.0.0.1	Netgear, Inc.	0x11 - Microso...	yes	yes	9/20/2012 14:22:55	9/20/20
✗	10.0.0.2	d0-67-e...	WIN-MSSELCK...	unknown	0x11 - Microso...	yes	no	9/20/2012 14:22:55	9/20/20
✗	10.0.0.3	00-15-5...	10.0.0.3	Microsoft Cor...	0x11 - Microso...	yes	yes	9/20/2012 14:25:06	9/20/20
✗	10.0.0.4	00-15-5...	Windows8	Microsoft Cor...	0x11 - Microso...	yes	yes	9/20/2012 14:25:08	9/20/20
✗	10.0.0.5	00-15-5...	10.0.0.5	Microsoft Cor...	0x11 - Microso...	yes	yes	9/20/2012 14:25:54	9/20/20
✗	10.0.0.6	00-15-5...	ADMIN-PC	Microsoft Cor...	0x11 - Microso...	yes	yes	9/20/2012 14:22:55	9/20/20
✓	10.0.0.7	d4-be-...	WIN-D39MR5...	unknown	0x11 - Microso...	yes	yes	9/20/2012 14:22:55	9/20/20
✓	10.0.0.8	00-15-5...	ADMIN	Microsoft Cor...	0x11 - Microso...	yes	yes	9/20/2012 14:22:55	9/20/20
✓	10.0.0.10	d4-be-...	WIN-2N9STOS...	unknown	0x11 - Microso...	yes	yes	9/20/2012 14:22:55	9/20/20
✓	10.0.0.12	00-15-5...	WINDOWS8	Microsoft Cor...	0x11 - Microso...	yes	yes	9/20/2012 14:22:55	9/20/20
✓	10.0.0.13	00-15-5...	WIN-EGBHISG...	Microsoft Cor...	0x11 - Microso...	yes	yes	9/20/2012 14:22:55	9/20/20

XArp 2.2.2 - 11 mappings - 2 interfaces - 25 alerts

FIGURE 7.6: XArp – ARP attacks detected

Lab Analysis

Analyze and document the results related to the lab exercise.

Tool/Utility	Information Collected/Objectives Achieved
XArp	**Interface [Ethernet]:** 0x11 **Source Mac:** d0-xx-xx-xx-xx-36 **Destination Mac:** 00-xx-xx-xx-xx-cc **Type [arp]:** 0x806 **Direction:** Out **Source IP:** 10.0.0.2 **Destination IP:** 10.0.0.1 **Host:** 10.0.0.1 **Vendor:** Netgear, Inc.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Determine how you can defend against ARP cache poisoning in a network.

Internet Connection Required	
☑ **Yes**	☐ No
Platform Supported	
☑ **Classroom**	☑ iLabs

Lab 8

Detecting Systems Running in Promiscuous Mode in a Network Using PromqryUI

PromqryUI is a tool with a Windows graphical interface that can be used to detect network interfaces that are running in promiscuous mode.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

With an ARP storm attack, an attacker collects the IP address and MAC address of the machines in a network for future attacks. An attacker can send ARP packets to attack a network. If an ARP packet with a forged gateway MAC address is pushed to the LAN, all communications within the LAN may fail. This attack uses all resources of both victim and non-victim computers.

As a network administrator you must always diagnose the network traffic using a network analyzer and configure routers to prevent ARP flooding. Using a specific technique with a protocol analyzer you should be able to identify the cause of the broadcast storm and a method to resolve the storm. Identify susceptible points on the network and protect them before attackers discover and exploit the vulnerabilities, especially on ARP-enabled LAN systems, a protocol with known security loopholes that allow attackers to conduct various ARP attacks.

Attackers may also install network interfaces to run in promiscuous mode to capture all the packets that pass over a network. As an expert **ethical hacker** and **penetration tester** you must be aware of the tools to detect network interfaces running in promiscuous mode as it might be a network sniffer. In this lab you will learn to use the tool PromqryUI to detect such network interfaces running in promiscuous mode.

Lab Objectives

The objective of this lab to accomplish:

- To detect promiscuous systems in a network

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 08 Sniffing

Lab Environment

To carry-out the lab, you need:

- **PromqryUI** is located at **D:\CEH-Tools\CEHv8 Module 08 Sniffing\Promiscuous Detection Tools\PromqryUI**
- You can also download the latest version of **PromqryUI** from http://www.microsoft.com/en-us/download/details.aspx?id=16883
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- A computer running **Windows 2008 Server**
- Administrative privileges to run tools

Lab Duration

Time: 10 Minutes

Overview of PromqryUI

PromqryUI can accurately determine if a modern managed Windows system has network interfaces in promiscuous mode. If a system has network interfaces in promiscuous mode, it may indicate the presence of a network sniffer running on the system.

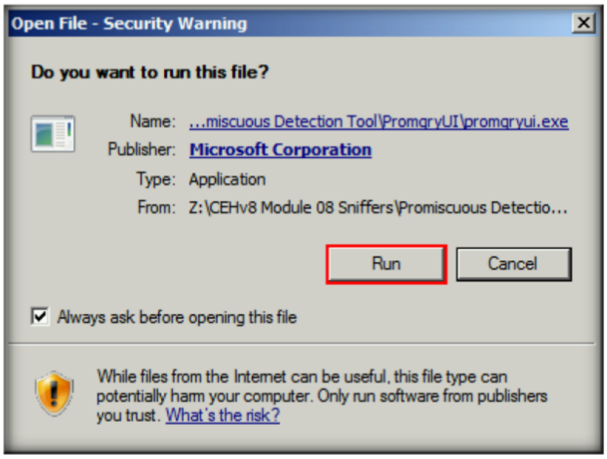
PromqryUI cannot detect standalone sniffers or sniffers running on non-Windows operating systems.

Lab Tasks

TASK 1

Running PromqryUI

1. Go to the tool location at **Z:\CEHv8 Module 08 Sniffing\Promiscuous Detection Tools\PromqryUI**.
2. Double-click **promqryui.exe**, and click **Run**.



Open File - Security Warning

Do you want to run this file?

Name: ...miscuous Detection Tool\PromqryUI\promqryui.exe

Publisher: Microsoft Corporation

Type: Application

From: Z:\CEHv8 Module 08 Sniffers\Promiscuous Detectio...

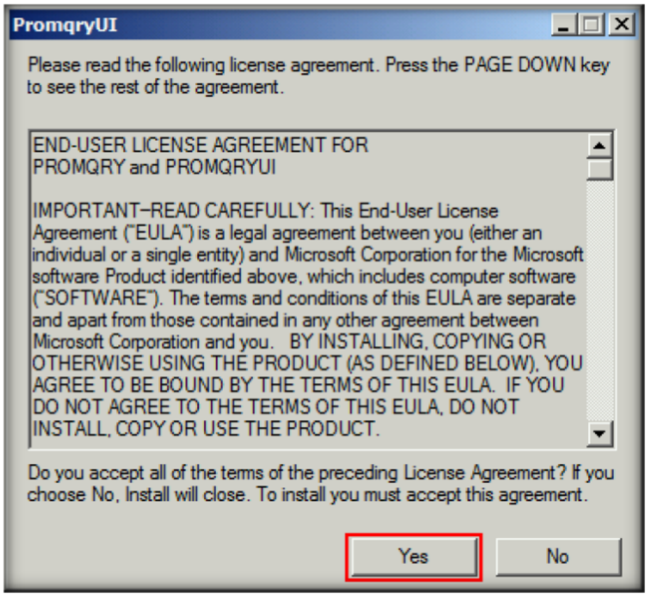
☑ Always ask before opening this file

While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you trust. What's the risk?

FIGURE 8.1: PromqryUI – Run prompt

3. Click **Yes** in the **PromqryUI License Agreement** window.

🗁 In a network, promiscuous mode allows a network device to intercept and read each network packet that arrives in its entirety.



Please read the following license agreement. Press the PAGE DOWN key to see the rest of the agreement.

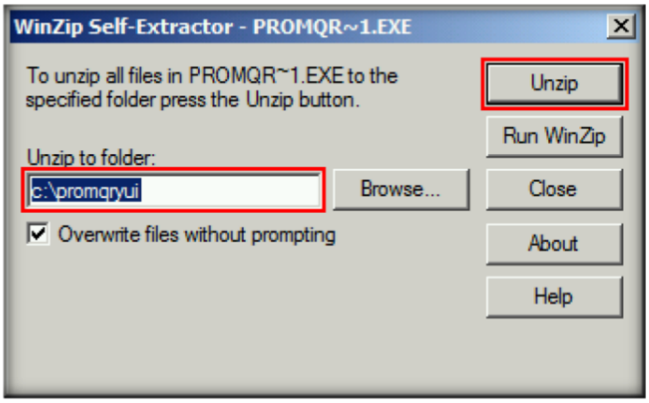
END-USER LICENSE AGREEMENT FOR
PROMQRY and PROMQRYUI

IMPORTANT–READ CAREFULLY: This End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and Microsoft Corporation for the Microsoft software Product identified above, which includes computer software ("SOFTWARE"). The terms and conditions of this EULA are separate and apart from those contained in any other agreement between Microsoft Corporation and you. BY INSTALLING, COPYING OR OTHERWISE USING THE PRODUCT (AS DEFINED BELOW), YOU AGREE TO BE BOUND BY THE TERMS OF THIS EULA. IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, DO NOT INSTALL, COPY OR USE THE PRODUCT.

Do you accept all of the terms of the preceding License Agreement? If you choose No, Install will close. To install you must accept this agreement.

FIGURE 8.2: PromqryUI – License Agreement dialog box

4. The **WinZip Self-Extractor** dialog box appears. Browse to a desired location (default location is **c:\promqryui**) to save the unzipped folder and click **Unzip**.



To unzip all files in PROMQR~1.EXE to the specified folder press the Unzip button.

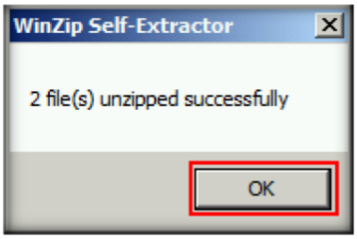
Unzip to folder: c:\promqryui

☑ Overwrite files without prompting

🗁 In a network, promiscuous mode allows a network device to intercept and read each network packet that arrives in its entirety.

FIGURE 8.3: PromqryUI – WinZip Self-Extractor dialog box

5. Click **OK** after the unzip is successful.

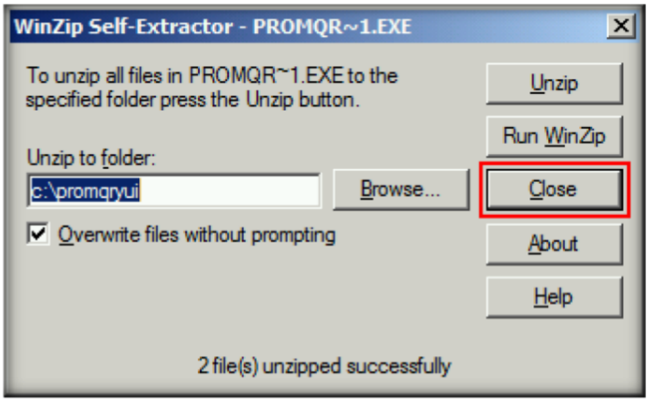


2 file(s) unzipped successfully

FIGURE 8.4: WinZip Self-Extractor dialog box

6. Now, click **Close** to close the **WinZip Self-Extractor** dialog box.

Unzip to folder allows you to browse and select a destination of your choice to save the setup file.



WinZip Self-Extractor - PROMQR~1.EXE

To unzip all files in PROMQR~1.EXE to the specified folder press the Unzip button.

Unzip to folder: c:\promqryui

☑ Overwrite files without prompting

2 file(s) unzipped successfully

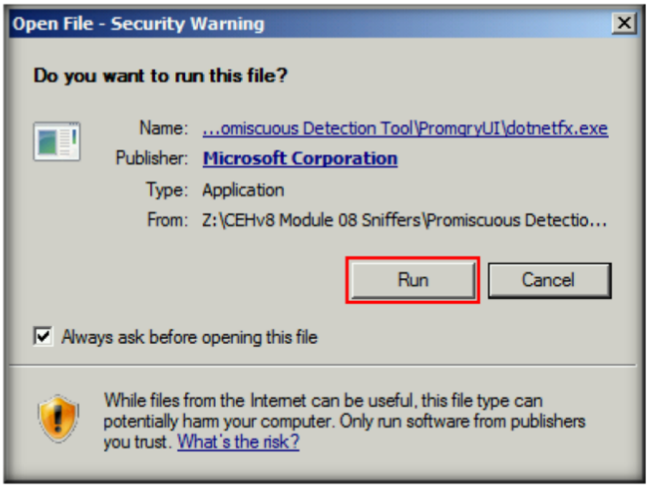
FIGURE 8.5: PromqryUI – WinZip Self-Extractor dialog box

7. Now, install **.NET Framework 1.1** by double-clicking the **dotnetfx.exe** file located at **Z:\CEHv8 Module 08 Sniffing\Promiscuous Detection Tools\PromqryUI**.

TASK 2

Running .NET Framework 1.1

8. Click **Run** in the **Open File - Security Warning** dialog box.



Open File - Security Warning

Do you want to run this file?

Name: ...omiscuous Detection Tool\PromqryUI\dotnetfx.exe
Publisher: Microsoft Corporation
Type: Application
From: Z:\CEHv8 Module 08 Sniffers\Promiscuous Detectio...

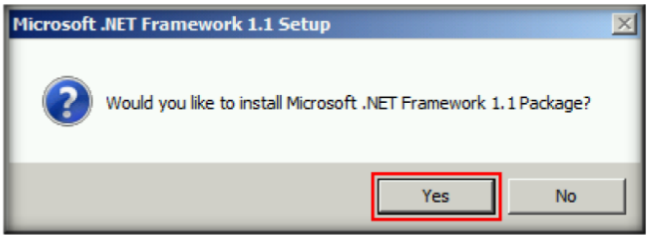
☑ Always ask before opening this file

While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you trust. What's the risk?

FIGURE 8.6: .NET Framework – Run dialog box

The .NET Framework version 1.1 redistributable package that includes everything you need to run applications developed using the .NET Framework.

9. Click **Yes** to initiate the .NET Framework installation in the **Setup** dialog box.

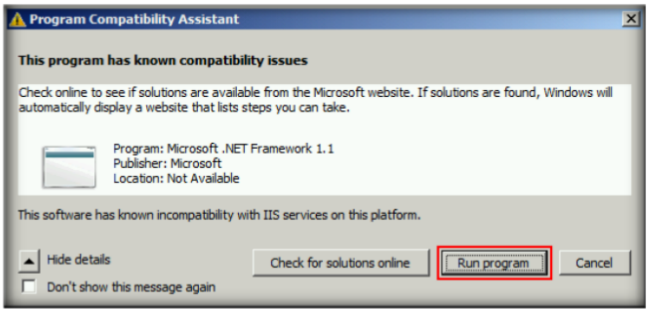


Microsoft .NET Framework 1.1 Setup

Would you like to install Microsoft .NET Framework 1.1 Package?

FIGURE 8.7: .NET Framework – Install dialog box

10. While attempting to install .NET Framework 1.1, you will get a **Program Compatibility Assistant** dialog box. Click **Run Program**.


Program Compatibility Assistant
Hide details
Don't show this message again
Check for solutions online
Run program
Cancel

This program has known compatibility issues

Check online to see if solutions are available from the Microsoft website. If solutions are found, Windows will automatically display a website that lists steps you can take.

Program: Microsoft .NET Framework 1.1
Publisher: Microsoft
Location: Not Available

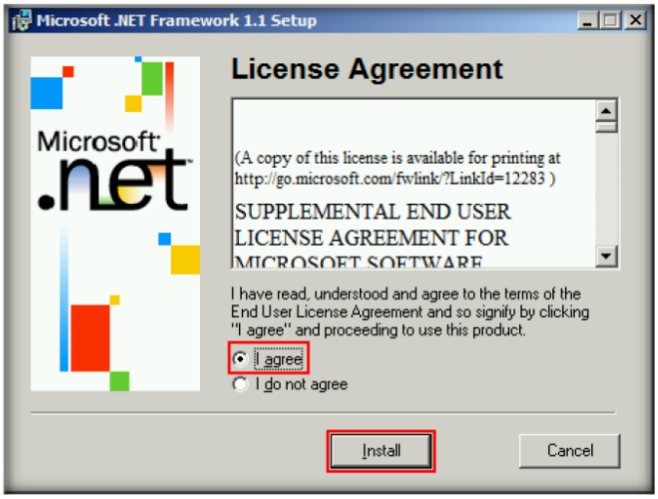
This software has known incompatibility with IIS services on this platform.

FIGURE 8.8: .NET Framework – Program Compatibility Assistant dialog box

TASK 3

Installing .NET Framework 1.1

11. Select the radio button for **I agree** and click **Install** in the **License Agreement** dialog box.


Microsoft .NET Framework 1.1 Setup
Microsoft
.net
License Agreement
Install
Cancel

(A copy of this license is available for printing at http://go.microsoft.com/fwlink/?LinkId=12283)

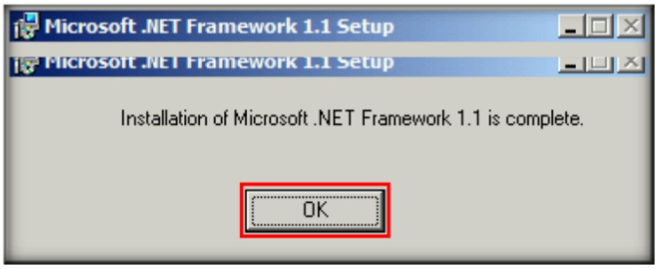
SUPPLEMENTAL END USER LICENSE AGREEMENT FOR MICROSOFT SOFTWARE

I have read, understood and agree to the terms of the End User License Agreement and so signify by clicking "I agree" and proceeding to use this product.

● I agree
○ I do not agree

FIGURE 8.9: .NET Framework – License Agreement dialog box

12. Once the installation is complete, click **OK** in the **Microsoft .NET Framework 1.1 Setup** dialog box.


Microsoft .NET Framework 1.1 Setup
Microsoft .NET Framework 1.1 Setup
OK

Installation of Microsoft .NET Framework 1.1 is complete.

FIGURE 8.10: .NET Framework – Installation complete message box

TASK 3

Installing PromqryUI

13. Now, go to **C:\promqryui** and double-click **pqsetup.msi** and follow the installation wizard to install PromqryUI.

14. Once installation is complete, go to **Start** and click **Promqry** to launch the program.

Promiscuous mode can be used in a malicious way to sniff on a network. In promiscuous mode, some software might send responses to frames even though they were addressed to another machine. However, experienced sniffers can prevent this by using carefully designed firewall settings.

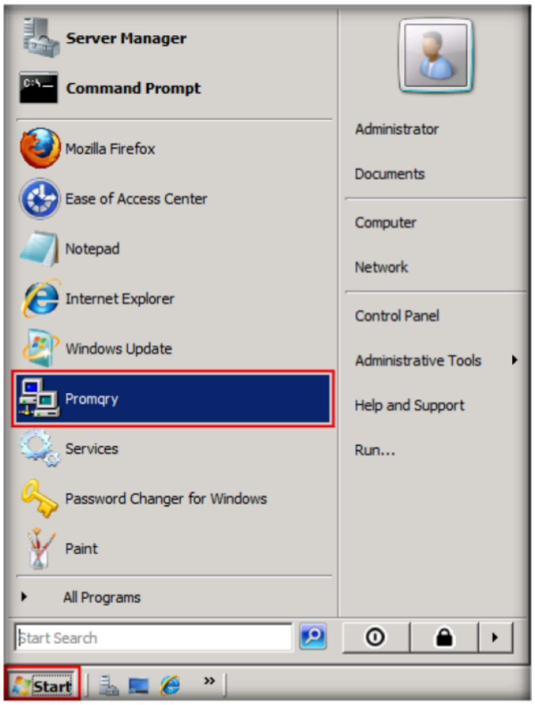

Server Manager
Command Prompt
Mozilla Firefox
Ease of Access Center
Notepad
Internet Explorer
Windows Update
Promqry
Services
Password Changer for Windows
Paint
All Programs
Administrator
Documents
Computer
Network
Control Panel
Administrative Tools
Help and Support
Run...
Start Search
Start

FIGURE 8.11: Windows 2008 Server – Start menu

15. The main window of PromqryUI appears. Click **Add**.

With the PromqryUI tool, you can add either a single system or multiple systems to query.

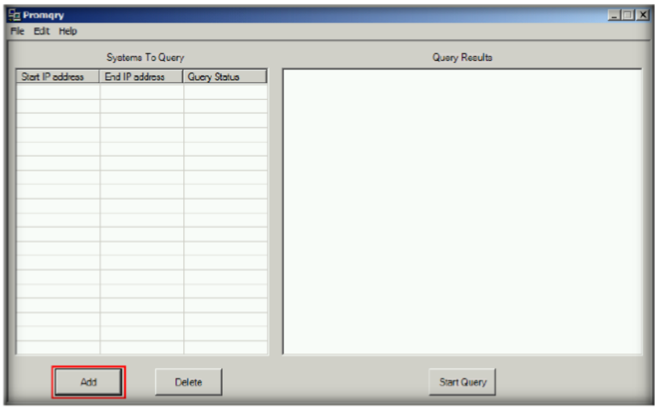

Promqry
File Edit Help
Systems To Query
Start IP address
End IP address
Query Status
Query Results
Add
Delete
Start Query

FIGURE 8.12: PromqryUI – Main window

16. The **Select Addition Type** dialog box will appear. Click **Add Single System**.

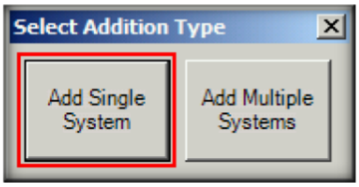
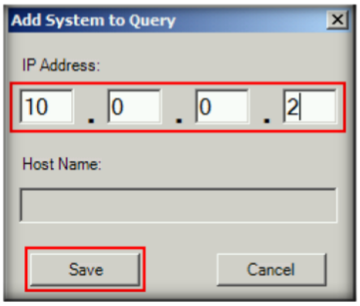

Select Addition Type
Add Single System
Add Multiple Systems

FIGURE 8.13: PromqryUI – Adding system

17. Type the IP address of the system you want to check for promiscuous mode in the **IP Address** field in the **Add System to Query** dialog box and click **Save**.


Add System to Query
Save
Cancel

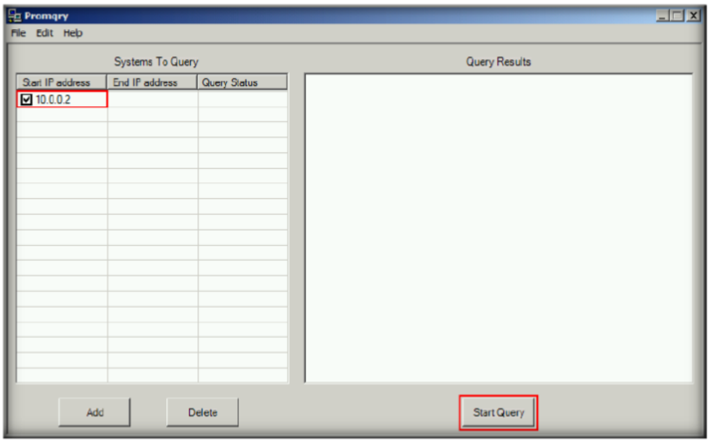
IP Address: 10 . 0 . 0 . 2

Host Name:

FIGURE 8.14: PromqryUI – Add System to Query

For systems that you need to query, a range of IP addresses can be provided. Also, you can just carry a query for a local system.

18. Select the added IP address in the **Systems To Query** section and click **Start Query**.

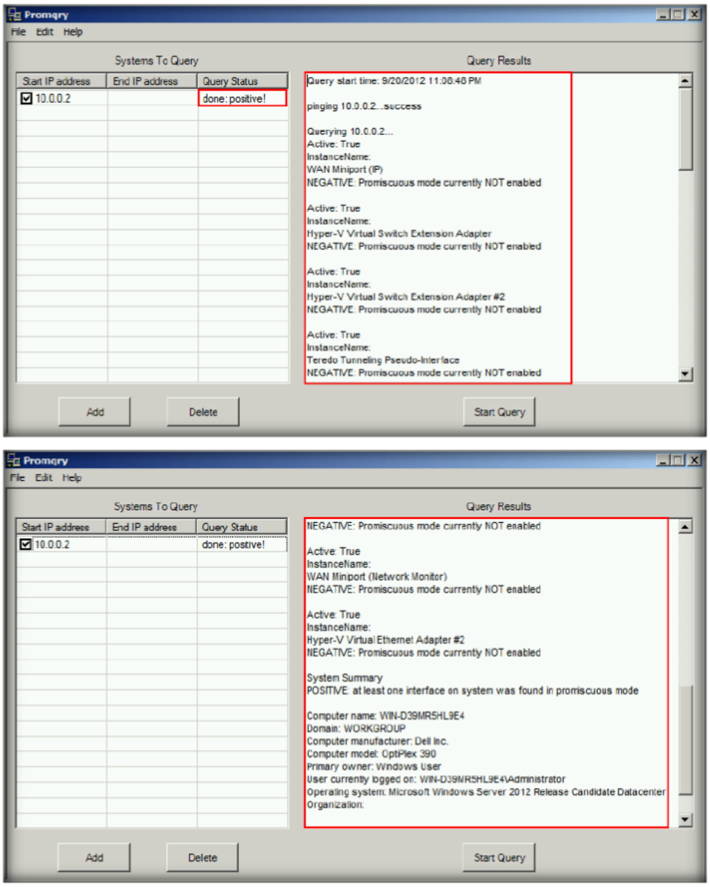

Promqry
File Edit Help
Systems To Query
Query Results
Add
Delete
Start Query

Start IP address	End IP address	Query Status
☑ 10.0.0.2		

FIGURE 8.15: PromqryUI – Querying system

19. Results will be displayed in **Query Results**.

Query results will let you know if the system is promiscuous mode or not and provides other information like Computer name, Domain, Computer Model, Manufacturer, Owner, etc.



Start IP address	End IP address	Query Status
☑ 10.0.0.2		done: positive!

```
Query start time: 9/20/2012 11:06:46 PM

pinging 10.0.0.2...success

Querying 10.0.0.2...
Active: True
InstanceName:
WAN Miniport (IP)
NEGATIVE: Promiscuous mode currently NOT enabled

Active: True
InstanceName:
Hyper-V Virtual Switch Extension Adapter
NEGATIVE: Promiscuous mode currently NOT enabled

Active: True
InstanceName:
Hyper-V Virtual Switch Extension Adapter #2
NEGATIVE: Promiscuous mode currently NOT enabled

Active: True
InstanceName:
Teredo Tunneling Pseudo-Interface
NEGATIVE: Promiscuous mode currently NOT enabled
```

Start IP address	End IP address	Query Status
☑ 10.0.0.2		done: postive!

```
NEGATIVE: Promiscuous mode currently NOT enabled

Active: True
InstanceName:
WAN Miniport (Network Monitor)
NEGATIVE: Promiscuous mode currently NOT enabled

Active: True
InstanceName:
Hyper-V Virtual Ethernet Adapter #2
NEGATIVE: Promiscuous mode currently NOT enabled

System Summary
POSITIVE: at least one interface on system was found in promiscuous mode

Computer name: WIN-D39MR5HL9E4
Domain: WORKGROUP
Computer manufacturer: Dell Inc.
Computer model: OptiPlex 390
Primary owner: Windows User
User currently logged on: WIN-D39MR5HL9E4\Administrator
Operating system: Microsoft Windows Server 2012 Release Candidate Datacenter
Organization:
```

FIGURE 8.16: PromqryUI – Query Results

Lab Analysis

Analyze and document the results related to the lab exercise.

Tool/Utility	Information Collected/Objectives Achieved
PromqryUI	**Computer name:** WIN-D39MR5HL9E4 **Domain:** WORKGROUP **Computer manufacturer:** Dell Inc. **Computer model:** OptiPlex 390 **Primary owner:** Windows User **User currently logged on:** WIN-D39MR5HL9E4\Administrator **Operating system:** Microsoft Windows Server 2012 Release Candidate Datacenter

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Determine how you can defend against ARP cache poisoning in a network

Internet Connection Required	
☑ **Yes**	☐ No
Platform Supported	
☑ **Classroom**	☑ iLabs

Lab 9

Sniffing Password from Captured Packets using Sniff – O – Matic

Sniff – O – Matic is a network protocol analyzer and packet sniffer with a clear and intuitive interface.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Attackers may install a sniffer in a trusted network to capture packets and will be able to view every single packet that is going across the network, if the network uses a hub or a router for data transmission. With the captured packets, attackers can learn about vulnerabilities and sniff the user name and password and log in to the network as an authenticated user. Once logged in successfully to a network, the hacker can easily install viruses and Trojans to steal data, sensitive information, and cause serious damage to that network.

As an expert **ethical hacker** and **penetration tester** you should have sound knowledge of sniffing, network protocols, and authentication mechanisms and encryption techniques. You should also regularly check your network and close the unnecessary ports that are open. Always ensure that if any sensitive data is required to be sent over the network, you use an encrypted protocol to minimize the data leakage.

Lab Objectives

The objective of this lab to sniff passwords using the tool Sniff – O – Matic through captured packets.

Lab Environment

To carry-out the lab, you need:

- **Sniff – O – Matic** is located at **D:\CEH-Tools\CEHv8 Module 08 Sniffing\Sniffing Tools\Sniff-O-Matic**
- You can also download the latest version of **Sniff – O – Matic** from http://www.kwakkelflap.com/sniffer.html

- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- A computer running **Windows Server 2012** as host machine
- Double-click **snifftrial.exe** and follow the wizard-driven installation steps to install **Sniff – O – Matic**
- Administrative privileges to run tools

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 08 Sniffing

Lab Duration

Time: 10 Minutes

Overview of Sniff – O – Matic

Sniff – O – Matic captures network traffic and enables you to analyze the data. Detailed packet information is available in a tree structure or a raw data view of the packet data. Sniff – O – Matic's button and columnar data display logically and succinctly presents the collected network traffic data.

Lab Tasks

1. Launch the **Start** menu by hovering the mouse cursor on the lower left corner of the desktop.

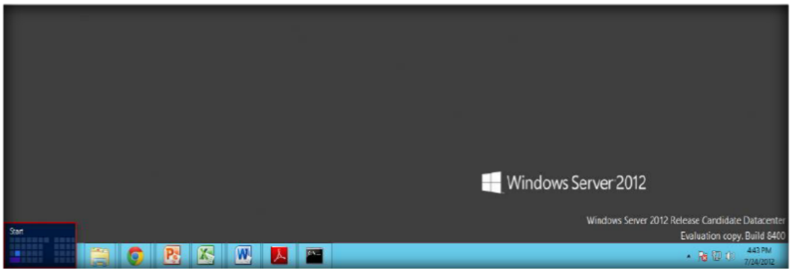

Windows Server 2012
Windows Server 2012 Release Candidate Datacenter
Evaluation copy. Build 8400
Start

FIGURE 9.1: Windows Server 2012 – Desktop view

TASK 1

Launching the Sniff-O-Matic tool

2. Click **Sniff – O – Matic** in the **Start** menu to launch the Sniff – O – Matic tool.

Sniff-O-Matic a packet sniffer is a computer program or a piece of computer hardware that can intercept and log traffic passing over a digital network or part of a network.

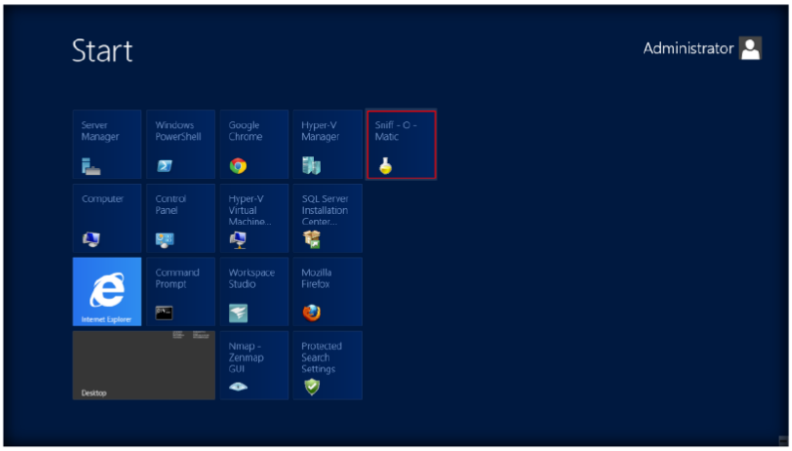

Start
Administrator
Server Manager
Windows PowerShell
Google Chrome
Hyper-V Manager
Sniff - O - Matic
Computer
Control Panel
Hyper-V Virtual Machine...
SQL Server Installation Center...
Internet Explorer
Command Prompt
Workspace Studio
Mozilla Firefox
Desktop
Nmap - Zenmap GUI
Protected Search Settings

FIGURE 9.2: Windows Server 2012 – Desktop view

3. The main **Sniff – O – Matic** window appears; select the adapter from the drop-down list and click the **Start Capture** ▶ button.

TASK 2

Sniff-O-Matic: Start Packet Capture

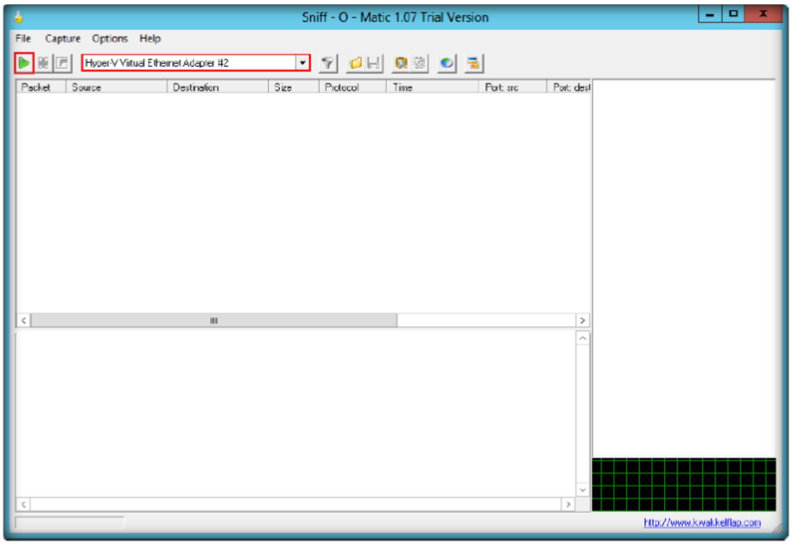
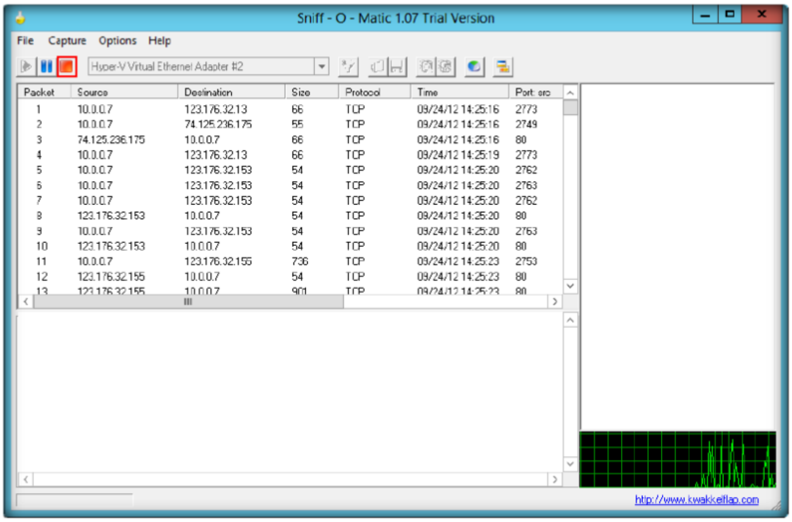

Sniff - O - Matic 1.07 Trial Version
File
Capture
Options
Help
Hyper-V Virtual Ethernet Adapter #2
Packet
Source
Destination
Size
Protocol
Time
Port: src
Port: dest
http://www.kwakkelflap.com

FIGURE 9.3: Sniff-O-Matic – Start capture

FIGURE 9.3: Sniff-O-Matic – Start capture

4. When the tool starts capturing the packets, launch a browser and log in to your email account.

5. Then, click the **Stop Capture** ■ button to view the captured packets.


Sniff - O - Matic 1.07 Trial Version
File
Capture
Options
Help
Hyper-V Virtual Ethernet Adapter #2
http://www.kwakkelflap.com

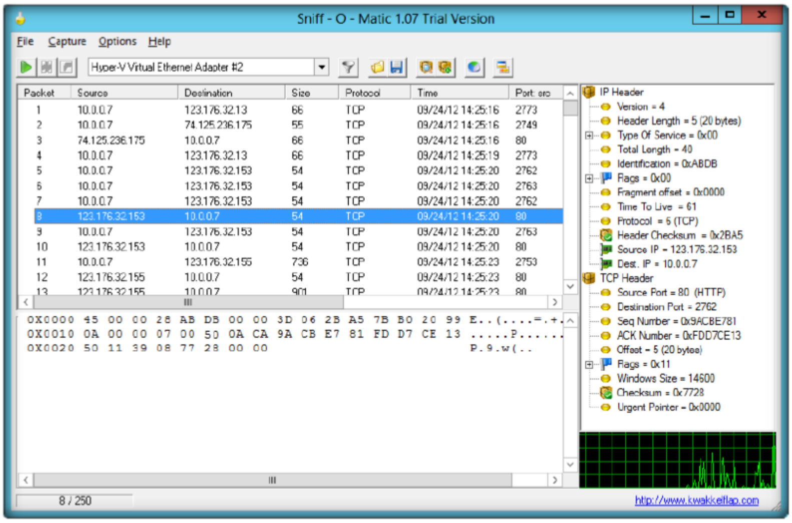
Packet	Source	Destination	Size	Protocol	Time	Port: src
1	10.0.0.7	123.176.32.13	66	TCP	09/24/12 14:25:16	2773
2	10.0.0.7	74.125.236.175	55	TCP	09/24/12 14:25:16	2749
3	74.125.236.175	10.0.0.7	66	TCP	09/24/12 14:25:16	80
4	10.0.0.7	123.176.32.13	66	TCP	09/24/12 14:25:19	2773
5	10.0.0.7	123.176.32.153	54	TCP	09/24/12 14:25:20	2762
6	10.0.0.7	123.176.32.153	54	TCP	09/24/12 14:25:20	2763
7	10.0.0.7	123.176.32.153	54	TCP	09/24/12 14:25:20	2762
8	123.176.32.153	10.0.0.7	54	TCP	09/24/12 14:25:20	80
9	10.0.0.7	123.176.32.153	54	TCP	09/24/12 14:25:20	2763
10	123.176.32.153	10.0.0.7	54	TCP	09/24/12 14:25:20	80
11	10.0.0.7	123.176.32.155	736	TCP	09/24/12 14:25:23	2753
12	123.176.32.155	10.0.0.7	54	TCP	09/24/12 14:25:23	80
13	123.176.32.155	10.0.0.7	901	TCP	09/24/12 14:25:23	80

🗁 Packet capture is the act of capturing data packets crossing a computer network.

FIGURE 9.4: Sniff-O-Matic – Stop capture

FIGURE 9.4: Sniff-O-Matic – Stop capture

6. In the list of captured packets, select a packet to view detailed information.


Sniff - O - Matic 1.07 Trial Version
File
Capture
Options
Help
Hyper-V Virtual Ethernet Adapter #2
8 / 250
http://www.kwakkelflap.com

Packet	Source	Destination	Size	Protocol	Time	Port: src
1	10.0.0.7	123.176.32.13	66	TCP	09/24/12 14:25:16	2773
2	10.0.0.7	74.125.236.175	55	TCP	09/24/12 14:25:16	2749
3	74.125.236.175	10.0.0.7	66	TCP	09/24/12 14:25:16	80
4	10.0.0.7	123.176.32.13	66	TCP	09/24/12 14:25:19	2773
5	10.0.0.7	123.176.32.153	54	TCP	09/24/12 14:25:20	2762
6	10.0.0.7	123.176.32.153	54	TCP	09/24/12 14:25:20	2763
7	10.0.0.7	123.176.32.153	54	TCP	09/24/12 14:25:20	2762
8	123.176.32.153	10.0.0.7	54	TCP	09/24/12 14:25:20	80
9	10.0.0.7	123.176.32.153	54	TCP	09/24/12 14:25:20	2763
10	123.176.32.153	10.0.0.7	54	TCP	09/24/12 14:25:20	80
11	10.0.0.7	123.176.32.155	736	TCP	09/24/12 14:25:23	2753
12	123.176.32.155	10.0.0.7	54	TCP	09/24/12 14:25:23	80
13	123.176.32.155	10.0.0.7	901	TCP	09/24/12 14:25:23	80

```
0X0000 45 00 00 28 AB DB 00 00 3D 06 2B A5 7B B0 20 99 E..(....=.+.
0X0010 0A 00 00 07 00 50 0A CA 9A CB E7 81 FD D7 CE 13 .....P......
0X0020 50 11 39 08 77 28 00 00                         P.9.w(..
```

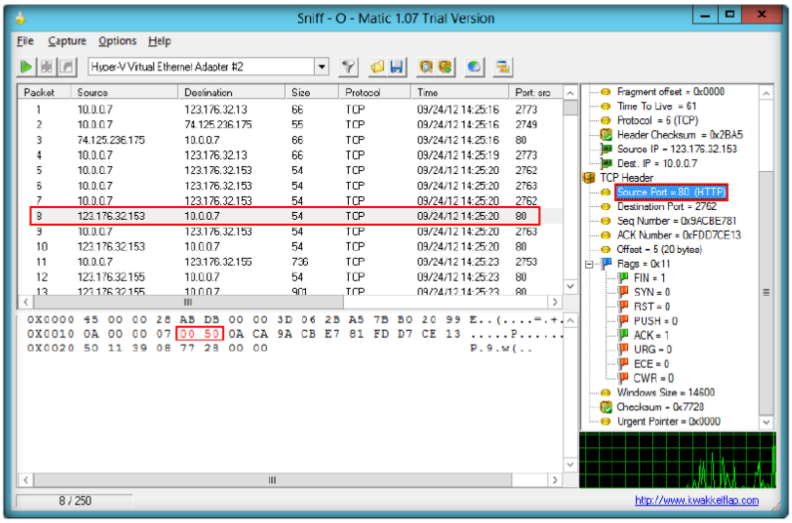
```
IP Header
  Version = 4
  Header Length = 5 (20 bytes)
  Type Of Service = 0x00
  Total Length = 40
  Identification = 0xABDB
  Flags = 0x00
  Fragment offset = 0x0000
  Time To Live  = 61
  Protocol  = 6 (TCP)
  Header Checksum  = 0x2BA5
  Source IP = 123.176.32.153
  Dest. IP = 10.0.0.7
TCP Header
  Source Port = 80  (HTTP)
  Destination Port = 2762
  Seq Number = 0x9ACBE781
  ACK Number = 0xFDD7CE13
  Offset = 5 (20 bytes)
  Flags = 0x11
  Windows Size = 14600
  Checksum = 0x7728
  Urgent Pointer = 0x0000
```

🗁 From the captured packets, detailed information such as Header Length, Protocol, Header Checksum, Source IP, Destination IP, etc. can be viewed by selecting a particular packet.

FIGURE 9.5: Sniff-O-Matic – Viewing packet information

FIGURE 9.5: Sniff-O-Matic – Viewing packet information

7. In the right pane, select items from the tree and the data for the respective item will be highlighted in red.


Sniff - O - Matic 1.07 Trial Version
File Capture Options Help
Hyper-V Virtual Ethernet Adapter #2
8 / 250
http://www.kwakkelflap.com

Packet	Source	Destination	Size	Protocol	Time	Port: src
1	10.0.0.7	123.176.32.13	66	TCP	09/24/12 14:25:16	2773
2	10.0.0.7	74.125.236.175	55	TCP	09/24/12 14:25:16	2749
3	74.125.236.175	10.0.0.7	66	TCP	09/24/12 14:25:16	80
4	10.0.0.7	123.176.32.13	66	TCP	09/24/12 14:25:19	2773
5	10.0.0.7	123.176.32.153	54	TCP	09/24/12 14:25:20	2762
6	10.0.0.7	123.176.32.153	54	TCP	09/24/12 14:25:20	2763
7	10.0.0.7	123.176.32.153	54	TCP	09/24/12 14:25:20	2762
8	123.176.32.153	10.0.0.7	54	TCP	09/24/12 14:25:20	80
9	10.0.0.7	123.176.32.153	54	TCP	09/24/12 14:25:20	2763
10	123.176.32.153	10.0.0.7	54	TCP	09/24/12 14:25:20	80
11	10.0.0.7	123.176.32.155	736	TCP	09/24/12 14:25:23	2753
12	123.176.32.155	10.0.0.7	54	TCP	09/24/12 14:25:23	80
13	123.176.32.155	10.0.0.7	901	TCP	09/24/12 14:25:23	80

```
0X0000 45 00 00 28 AB DB 00 00 3D 06 2B A5 7B B0 20 99 E..(.....=.+.
0X0010 0A 00 00 07 00 50 0A CA 9A CB E7 81 FD D7 CE 13 .....P......
0X0020 50 11 39 08 77 28 00 00                         P.9.w(..
```

- Fragment offset = 0x0000
- Time To Live = 61
- Protocol = 6 (TCP)
- Header Checksum = 0x2BA5
- Source IP = 123.176.32.153
- Dest. IP = 10.0.0.7
- TCP Header
  - Source Port = 80 (HTTP)
  - Destination Port = 2762
  - Seq Number = 0x9ACBE781
  - ACK Number = 0xFDD7CE13
  - Offset = 5 (20 bytes)
  - Flags = 0x11
    - FIN = 1
    - SYN = 0
    - RST = 0
    - PUSH = 0
    - ACK = 1
    - URG = 0
    - ECE = 0
    - CWR = 0
  - Windows Size = 14600
  - Checksum = 0x7728
  - Urgent Pointer = 0x0000

FIGURE 9.6: Sniff-O-Matic – Viewing packet information

Port numbers can occasionally be seen in a web or other service. By default, HTTP uses port 80 and HTTPS uses port 443, but a URL - http://www.example.com:8080/path/ specifies that the web resource be served by the HTTP server on port 8080

8. Now, perform a search for the data in captured frames. Select **Options → Find**.

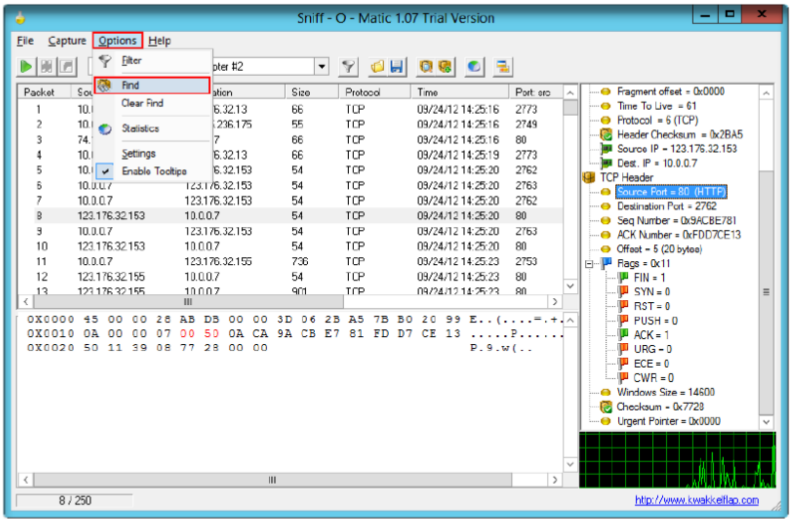
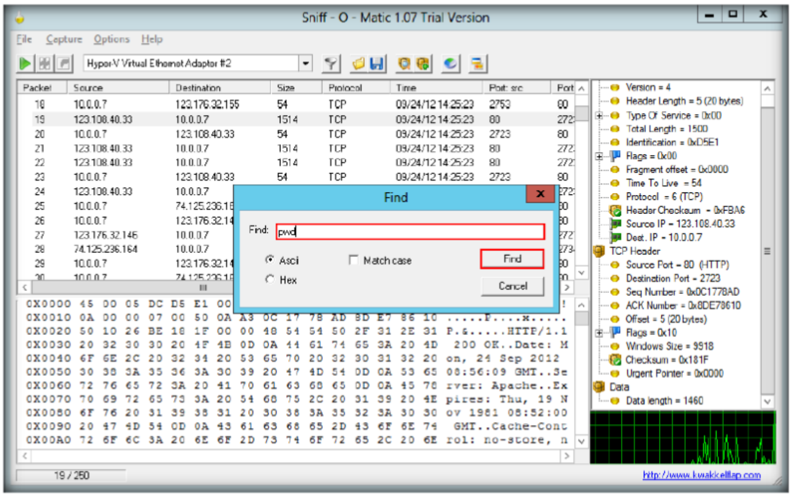

Sniff - O - Matic 1.07 Trial Version
File Capture Options Help
Filter
Find
Clear Find
Statistics
Settings
Enable Tooltips
8 / 250
http://www.kwakkelflap.com

FIGURE 9.7: Sniff-O-Matic – Performing search

FIGURE 9.7: Sniff-O-Matic – Performing search

9. The **Find** pop-up box appears; type **pwd** to search for the password information.

🗁 Detailed packet information is available in a tree structure or a raw data view of the packet data.



Sniff - O - Matic 1.07 Trial Version
File
Capture
Options
Help
HyperV Virtual Ethernet Adapter #2

Packet	Source	Destination	Size	Protocol	Time	Port: src	Port
18	10.0.0.7	123.176.32.155	54	TCP	09/24/12 14:25:23	2753	80
19	123.108.40.33	10.0.0.7	1514	TCP	09/24/12 14:25:23	80	272
20	10.0.0.7	123.108.40.33	54	TCP	09/24/12 14:25:23	2723	80
21	123.108.40.33	10.0.0.7	1514	TCP	09/24/12 14:25:23	80	272
22	123.108.40.33	10.0.0.7	1514	TCP	09/24/12 14:25:23	80	272
23	10.0.0.7	123.108.40.33	54	TCP	09/24/12 14:25:23	2723	80
24	123.108.40.33	10.0.0.7					272
25	10.0.0.7	74.125.236.1					80
26	10.0.0.7	123.176.32.14					80
27	123.176.32.146	10.0.0.7					272
28	74.125.236.164	10.0.0.7					273
29	10.0.0.7	123.176.32.14					80
30	10.0.0.7	74.125.236.1					80

Find

Find: pwd

● Asci ☐ Match case Find
○ Hex Cancel

```
0X0000 45 00 05 DC D5 E1 00                                                !
0X0010 0A 00 00 07 00 50 0A A3 0C 17 78 AD 8D E7 86 10 .....P....x.....
0X0020 50 10 26 BE 18 1F 00 00 48 54 54 50 2F 31 2E 31 P.&.....HTTP/1.1
0X0030 20 32 30 30 20 4F 4B 0D 0A 44 61 74 65 3A 20 4D  200 OK..Date: M
0X0040 6F 6E 2C 20 32 34 20 53 65 70 20 32 30 31 32 20 on, 24 Sep 2012
0X0050 30 38 3A 35 36 3A 30 39 20 47 4D 54 0D 0A 53 65 08:56:09 GMT..Se
0X0060 72 76 65 72 3A 20 41 70 61 63 68 65 0D 0A 45 78 rver: Apache..Ex
0X0070 70 69 72 65 73 3A 20 54 68 75 2C 20 31 39 20 4E pires: Thu, 19 N
0X0080 6F 76 20 31 39 38 31 20 30 38 3A 35 32 3A 30 30 ov 1981 08:52:00
0X0090 20 47 4D 54 0D 0A 43 61 63 68 65 2D 43 6F 6E 74  GMT..Cache-Cont
0X00A0 72 6F 6C 3A 20 6E 6F 2D 73 74 6F 72 65 2C 20 6E rol: no-store, n
```

```
Version = 4
Header Length = 5 (20 bytes)
Type Of Service = 0x00
Total Length = 1500
Identification = 0xD5E1
Flags = 0x00
Fragment offset = 0x0000
Time To Live  = 54
Protocol  = 6 (TCP)
Header Checksum  - 0xFBA6
Source IP - 123.108.40.33
Dest. IP - 10.0.0.7
TCP Header
Source Port - 80  (HTTP)
Destination Port - 2723
Seq Number = 0x0C1778AD
ACK Number = 0x8DE78610
Offset = 5 (20 bytes)
Flags = 0x10
Windows Size = 9918
Checksum = 0x181F
Urgent Pointer = 0x0000
Data
Data length = 1460
```

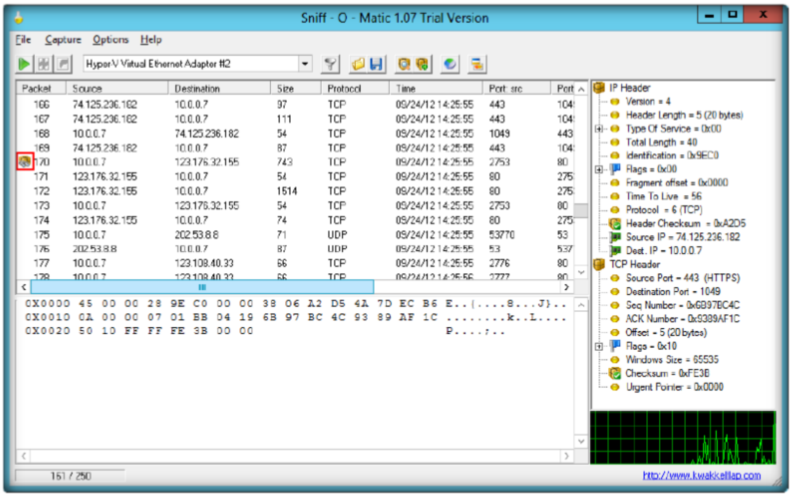
FIGURE 9.8: Sniff-O-Matic – Performing password search

FIGURE 9.8: Sniff-O-Matic – Performing password search

10. An icon 🔍 (packets with binoculars) will appear for the found packets, as shown in the following screenshot.

🗁 Sniff-O-Matic's key features include:

- Capture IP packets on your LAN without packet loss
- Monitor network activity in real time
- Filters to show only the packets you want
- Real-time checksum calculation
- Save and load captured packets
- Auto start capturing and continuous capture
- Traffic charts with filter info



Sniff - O - Matic 1.07 Trial Version
File
Capture
Options
Help
HyperV Virtual Ethernet Adapter #2

Packet	Source	Destination	Size	Protocol	Time	Port: src	Port
166	74.125.236.182	10.0.0.7	97	TCP	09/24/12 14:25:55	443	104
167	74.125.236.182	10.0.0.7	111	TCP	09/24/12 14:25:55	443	104
168	10.0.0.7	74.125.236.182	54	TCP	09/24/12 14:25:55	1049	443
169	74.125.236.182	10.0.0.7	87	TCP	09/24/12 14:25:55	443	104
170	10.0.0.7	123.176.32.155	743	TCP	09/24/12 14:25:55	2753	80
171	123.176.32.155	10.0.0.7	54	TCP	09/24/12 14:25:55	80	275
172	123.176.32.155	10.0.0.7	1514	TCP	09/24/12 14:25:55	80	275
173	10.0.0.7	123.176.32.155	54	TCP	09/24/12 14:25:55	2753	80
174	123.176.32.155	10.0.0.7	74	TCP	09/24/12 14:25:55	80	275
175	10.0.0.7	202.53.8.8	71	UDP	09/24/12 14:25:55	53770	53
176	202.53.8.8	10.0.0.7	87	UDP	09/24/12 14:25:55	53	537
177	10.0.0.7	123.108.40.33	66	TCP	09/24/12 14:25:55	2776	80
178	10.0.0.7	123.108.40.33	66	TCP	09/24/12 14:25:56	2777	80

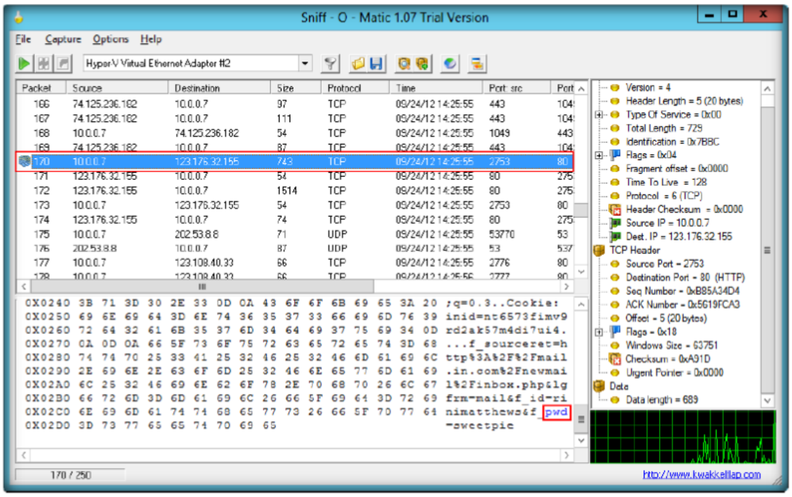
```
0X0000 45 00 00 28 9E C0 00 00 38 06 A2 D5 4A 7D EC B6 E..(....8...J}..
0X0010 0A 00 00 07 01 BB 04 19 6B 97 BC 4C 93 89 AF 1C ........k..L....
0X0020 50 10 FF FF FE 3B 00 00                         P....;..
```

```
IP Header
Version = 4
Header Length = 5 (20 bytes)
Type Of Service = 0x00
Total Length = 40
Identification = 0x9EC0
Flags = 0x00
Fragment offset = 0x0000
Time To Live  = 56
Protocol  = 6 (TCP)
Header Checksum  = 0xA2D5
Source IP = 74.125.236.182
Dest. IP - 10.0.0.7
TCP Header
Source Port - 443  (HTTPS)
Destination Port - 1049
Seq Number - 0x6B97BC4C
ACK Number - 0x9389AF1C
Offset - 5 (20 bytes)
Flags - 0x10
Windows Size = 65535
Checksum = 0xFE3B
Urgent Pointer = 0x0000
```

FIGURE 9.9: Sniff-O-Matic – Password search results

11. Select the found packet and scroll down the data list for the information, which will be indicated in blue.

Packets captured using Sniff-O-Matic allows you to sniff the password available in cleartext format. If an attacker is able to capture these packets, he can easily identify the password and login to the network as an authenticated user. Attackers will have an advantage if they discover the same password is being used for all the computers.


Sniff - O - Matic 1.07 Trial Version
File
Capture
Options
Help
Hyper-V Virtual Ethernet Adapter #2
170 / 250
http://www.kwakkelflap.com

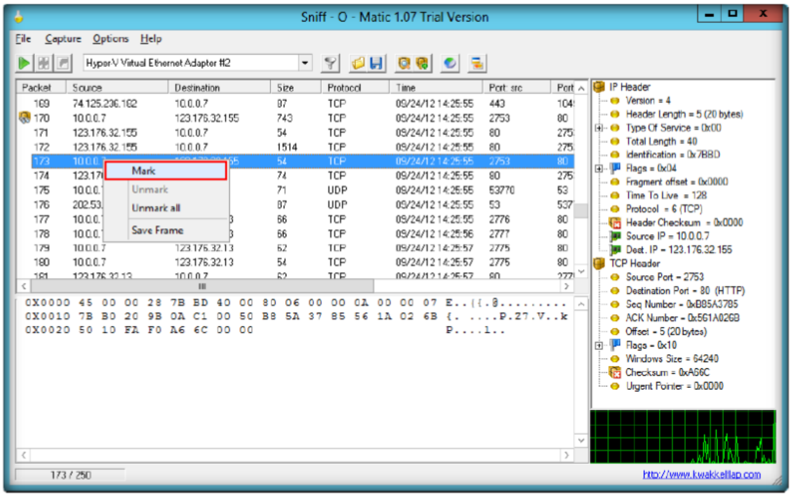
Packet	Source	Destination	Size	Protocol	Time	Port src	Port
166	74.125.236.182	10.0.0.7	97	TCP	09/24/12 14:25:55	443	104
167	74.125.236.182	10.0.0.7	111	TCP	09/24/12 14:25:55	443	104
168	10.0.0.7	74.125.236.182	54	TCP	09/24/12 14:25:55	1049	443
169	74.125.236.182	10.0.0.7	87	TCP	09/24/12 14:25:55	443	104
170	10.0.0.7	123.176.32.155	743	TCP	09/24/12 14:25:55	2753	80
171	123.176.32.155	10.0.0.7	54	TCP	09/24/12 14:25:55	80	275
172	123.176.32.155	10.0.0.7	1514	TCP	09/24/12 14:25:55	80	275
173	10.0.0.7	123.176.32.155	54	TCP	09/24/12 14:25:55	2753	80
174	123.176.32.155	10.0.0.7	74	TCP	09/24/12 14:25:55	80	275
175	10.0.0.7	202.53.8.8	71	UDP	09/24/12 14:25:55	53770	53
176	202.53.8.8	10.0.0.7	87	UDP	09/24/12 14:25:55	53	537
177	10.0.0.7	123.108.40.33	66	TCP	09/24/12 14:25:55	2776	80

```
0X0240 3B 71 3D 30 2E 33 0D 0A 43 6F 6F 6B 69 65 3A 20 ;q=0.3..Cookie:
0X0250 69 6E 69 64 3D 6E 74 36 35 37 33 66 69 6D 76 39 inid=nt6573fimv9
0X0260 72 64 32 61 6B 35 37 6D 34 64 69 37 75 69 34 0D rd2ak57m4di7ui4.
0X0270 0A 0D 0A 66 5F 73 6F 75 72 63 65 72 65 74 3D 68 ...f_sourceret=h
0X0280 74 74 70 25 33 41 25 32 46 25 32 46 6D 61 69 6C ttp%3A%2F%2Fmail
0X0290 2E 69 6E 2E 63 6F 6D 25 32 46 6E 65 77 6D 61 69 .in.com%2Fnewmai
0X02A0 6C 25 32 46 69 6E 62 6F 78 2E 70 68 70 26 6C 67 l%2Finbox.php&lg
0X02B0 66 72 6D 3D 6D 61 69 6C 26 66 5F 69 64 3D 72 69 frm=mail&f_id=ri
0X02C0 6E 69 6D 61 74 74 68 65 77 73 26 66 5F 70 77 64 nimatthews&f_pwd
0X02D0 3D 73 77 65 65 74 70 69 65                      =sweetpie
```

```
Version = 4
Header Length = 5 (20 bytes)
Type Of Service = 0x00
Total Length = 729
Identification = 0x7BBC
Flags = 0x04
Fragment offset = 0x0000
Time To Live  = 128
Protocol  = 6 (TCP)
Header Checksum  = 0x0000
Source IP = 10.0.0.7
Dest. IP = 123.176.32.155
TCP Header
Source Port = 2753
Destination Port = 80  (HTTP)
Seq Number = 0xB85A34D4
ACK Number = 0x5619FCA3
Offset = 5 (20 bytes)
Flags = 0x18
Windows Size = 63751
Checksum = 0xA91D
Urgent Pointer = 0x0000
Data
Data length = 689
```

FIGURE 9.10: Sniff-O-Matic – Password search results

12. To mark the packets, right-click the selected packet and click **Mark**.


Sniff - O - Matic 1.07 Trial Version
File
Capture
Options
Help
Hyper-V Virtual Ethernet Adapter #2
Mark
Unmark
Unmark all
Save Frame
173 / 250
http://www.kwakkelflap.com

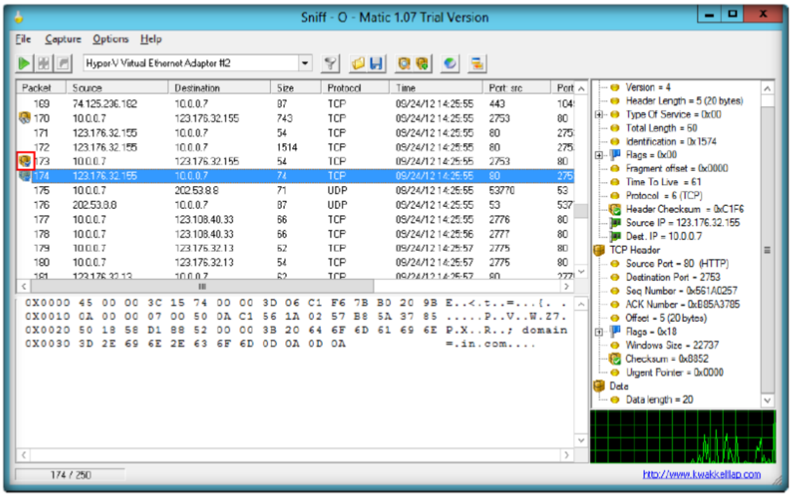
Packet	Source	Destination	Size	Protocol	Time	Port src	Port
169	74.125.236.182	10.0.0.7	87	TCP	09/24/12 14:25:55	443	104
170	10.0.0.7	123.176.32.155	743	TCP	09/24/12 14:25:55	2753	80
171	123.176.32.155	10.0.0.7	54	TCP	09/24/12 14:25:55	80	275
172	123.176.32.155	10.0.0.7	1514	TCP	09/24/12 14:25:55	80	275
173	10.0.0.	55	54	TCP	09/24/12 14:25:55	2753	80
174	123.17		74	TCP	09/24/12 14:25:55	80	275
175	10.0.0.		71	UDP	09/24/12 14:25:55	53770	53
176	202.53.		87	UDP	09/24/12 14:25:55	53	537
177	10.0.0.	3	66	TCP	09/24/12 14:25:55	2776	80
178	10.0.0.	3	66	TCP	09/24/12 14:25:56	2777	80
179	10.0.0.7	123.176.32.13	62	TCP	09/24/12 14:25:57	2775	80
180	10.0.0.7	123.176.32.13	54	TCP	09/24/12 14:25:57	2775	80

```
0X0000 45 00 00 28 7B BD 40 00 80 06 00 00 0A 00 00 07 E..({.@.........
0X0010 7B B0 20 9B 0A C1 00 50 B8 5A 37 85 56 1A 02 6B {. ....P.Z7.V..k
0X0020 50 10 FA F0 A6 6C 00 00                         P....l..
```

```
IP Header
Version = 4
Header Length = 5 (20 bytes)
Type Of Service = 0x00
Total Length = 40
Identification = 0x7BBD
Flags = 0x04
Fragment offset = 0x0000
Time To Live  = 128
Protocol  = 6 (TCP)
Header Checksum  = 0x0000
Source IP = 10.0.0.7
Dest. IP = 123.176.32.155
TCP Header
Source Port = 2753
Destination Port = 80  (HTTP)
Seq Number = 0xB85A3785
ACK Number = 0x561A026B
Offset = 5 (20 bytes)
Flags = 0x10
Windows Size = 64240
Checksum = 0xA66C
Urgent Pointer = 0x0000
```

FIGURE 9.11: Sniff-O-Matic – Marking a packet

13. Once the packets are marked, they will have a different icon.


Sniff - O - Matic 1.07 Trial Version
File
Capture
Options
Help
HyperV Virtual Ethernet Adapter #2
http://www.kwakkelflap.com
174 / 250

Packet	Source	Destination	Size	Protocol	Time	Port src	Port
169	74.125.236.182	10.0.0.7	87	TCP	09/24/12 14:25:55	443	104
170	10.0.0.7	123.176.32.155	743	TCP	09/24/12 14:25:55	2753	80
171	123.176.32.155	10.0.0.7	54	TCP	09/24/12 14:25:55	80	275
172	123.176.32.155	10.0.0.7	1514	TCP	09/24/12 14:25:55	80	275
173	10.0.0.7	123.176.32.155	54	TCP	09/24/12 14:25:55	2753	80
174	123.176.32.155	10.0.0.7	74	TCP	09/24/12 14:25:55	80	275
175	10.0.0.7	202.53.8.8	71	UDP	09/24/12 14:25:55	53770	53
176	202.53.8.8	10.0.0.7	87	UDP	09/24/12 14:25:55	53	537
177	10.0.0.7	123.108.40.33	66	TCP	09/24/12 14:25:55	2776	80
178	10.0.0.7	123.108.40.33	66	TCP	09/24/12 14:25:56	2777	80
179	10.0.0.7	123.176.32.13	62	TCP	09/24/12 14:25:57	2775	80
180	10.0.0.7	123.176.32.13	54	TCP	09/24/12 14:25:57	2775	80

```
0X0000 45 00 00 3C 15 74 00 00 3D 06 C1 F6 7B B0 20 9B E..<.t..=...{. .
0X0010 0A 00 00 07 00 50 0A C1 56 1A 02 57 B8 5A 37 85 .....P..V..W.Z7.
0X0020 50 18 58 D1 88 52 00 00 3B 20 64 6F 6D 61 69 6E P.X..R..; domain
0X0030 3D 2E 69 6E 2E 63 6F 6D 0D 0A 0D 0A             =.in.com....
```

```
Version = 4
Header Length = 5 (20 bytes)
Type Of Service = 0x00
Total Length = 60
Identification = 0x1574
Flags = 0x00
Fragment offset = 0x0000
Time To Live  = 61
Protocol  = 6 (TCP)
Header Checksum  = 0xC1F6
Source IP = 123.176.32.155
Dest. IP = 10.0.0.7
TCP Header
  Source Port - 80  (HTTP)
  Destination Port - 2753
  Seq Number - 0x561A0257
  ACK Number - 0xB85A3785
  Offset - 5 (20 bytes)
  Flags - 0x18
  Windows Size - 22737
  Checksum = 0x8852
  Urgent Pointer = 0x0000
Data
  Data length = 20
```

FIGURE 9.12: Sniff-O-Matic – Marked packets

One of the features of the tool includes, protocol and port data, the program displays source and destination IP addresses, and raw packet information. The program offers no IP address to domain name conversion..

Lab Analysis

Analyze and document the results related to the lab exercise.

Tool/Utility	Information Collected/Objectives Achieved
Sniff-O-Matic	**Header Length:** 5 **Time To Live:** 61 **Protocol:** 6 **Header Checksum:** 0xC1F6 **Source IP:** 123.176.32.155 **Dest. IP:** 10.0.0.7 **Source Port:** 80 (HTTP) **Destination Port:** 2753 **Username and password**

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Determine how you can defend against ARP cache poisoning in a network.

Internet Connection Required	
☑ **Yes**	☐ No
Platform Supported	
☑ **Classroom**	☑ iLabs